U.S. Department of Justice
Federal Bureau of Investigation

*Report to
the National Commission
on Terrorist Attacks upon the
United States:*

The FBI's Counterterrorism Program
Since September 2001

April 14, 2004

Report to

The National Commission on Terrorist Attacks upon the United States

The FBI's Counterterrorism Program

Since September 2001

TABLE OF CONTENTS

Executive Summary

Since the horrific attacks of September 11, 2001, the men and women of the Federal Bureau of Investigation (*FBI*) have implemented a comprehensive plan that fundamentally transforms the organization to enhance our ability to predict and prevent terrorism. We overhauled our counterterrorism operations, expanded our intelligence capabilities, modernized our business practices and technology, and improved coordination with our partners.

Our plan consists of seven basic elements:

1 Prioritization

We replaced a priority system that allowed supervisors a great deal of flexibility with a set of 10 priorities that strictly govern the allocation of personnel and resources in every FBI program and field office. Counterterrorism is now our overriding priority, and every terrorism lead is addressed, even if it requires a diversion of resources from other priority areas.

2 Mobilization

To implement these new priorities, we increased the number of Special Agents assigned to terrorism matters and hired hundreds of intelligence analysts and translators. We also established a number of operational units that give us new or improved capabilities to address the terrorist threat. These include the 24/7 Counterterrorism Watch and the National Joint Terrorism Task Force to manage and share threat information; the Terrorism Financing Operation Section to centralize efforts to stop terrorist financing; document/media exploitation squads to exploit material found overseas for its intelligence value; deployable "Fly Teams" to lend counterterrorism expertise wherever it is needed; and the Terrorist Screening Center and Foreign Terrorist Tracking Task Force to help identify terrorists and keep them out of the United States *(U.S.)*.

3 Centralization

We centralized management of our Counterterrorism Program at Headquarters to limit "stove-piping" of information, to ensure consistency of counterterrorism priorities and strategy across the organization, to integrate counterterrorism operations here and overseas, to improve coordination with other agencies and governments, and to make senior managers accountable for the overall development and success of our counterterrorism efforts.

4 Intelligence Integration

We are building an enterprise-wide intelligence program that has substantially improved our ability to strategically direct our intelligence collection and to fuse, analyze, and disseminate our terrorism-related intelligence. After the USA PATRIOT Act, related Attorney General Guidelines, and the ensuing opinion by the Foreign Intelligence Surveillance Court of Review removed the barrier to sharing information between intelligence and criminal investigations, we quickly implemented a plan to integrate all our capabilities to better prevent terrorist attacks. We then

elevated intelligence to program-level status, putting in place a formal structure and concepts of operations to govern FBI-wide intelligence functions, and establishing Field Intelligence Groups in every field office. We recently issued a series of new procedures that fundamentally transform our approach to hiring, training, and career development to cultivate and instill a capacity and understanding of intelligence processes and objectives within the entire Bureau workforce.

5 Coordination

Understanding that we cannot defeat terrorism without strong partnerships, we have enhanced the level of coordination and information sharing with state and municipal law enforcement personnel. We expanded the number of Joint Terrorism Task Forces, increased technological connectivity with our partners, and implemented new ways of sharing information through vehicles such as the Intelligence Bulletin, the Alert System, and the Terrorist Screening Center. To improve coordination with other federal agencies and members of the Intelligence Community, we joined with our federal partners to establish the Terrorist Threat Integration Center, exchanged personnel, instituted joint briefings, and started using secure networks to share information. We also improved our relationships with foreign governments by building on the overseas expansion started under Director Louis Freeh; by offering investigative and forensic support and training; and by working together on task forces and joint operations. Finally, we expanded outreach to minority communities, and improved coordination with private businesses involved in critical infrastructure and finance.

6 Information Technology

We are making substantial progress in upgrading our information technology to streamline our business processes and to improve our ability to search for and analyze information, draw connections, and share it both inside the Bureau and out. We deployed a secure high-speed network, put new or upgraded computers on desktops, and consolidated terrorist information in a searchable central database. We developed, and are preparing to launch, the Virtual Case File, a state-of-the-art case management system that will revolutionize how the FBI does business.

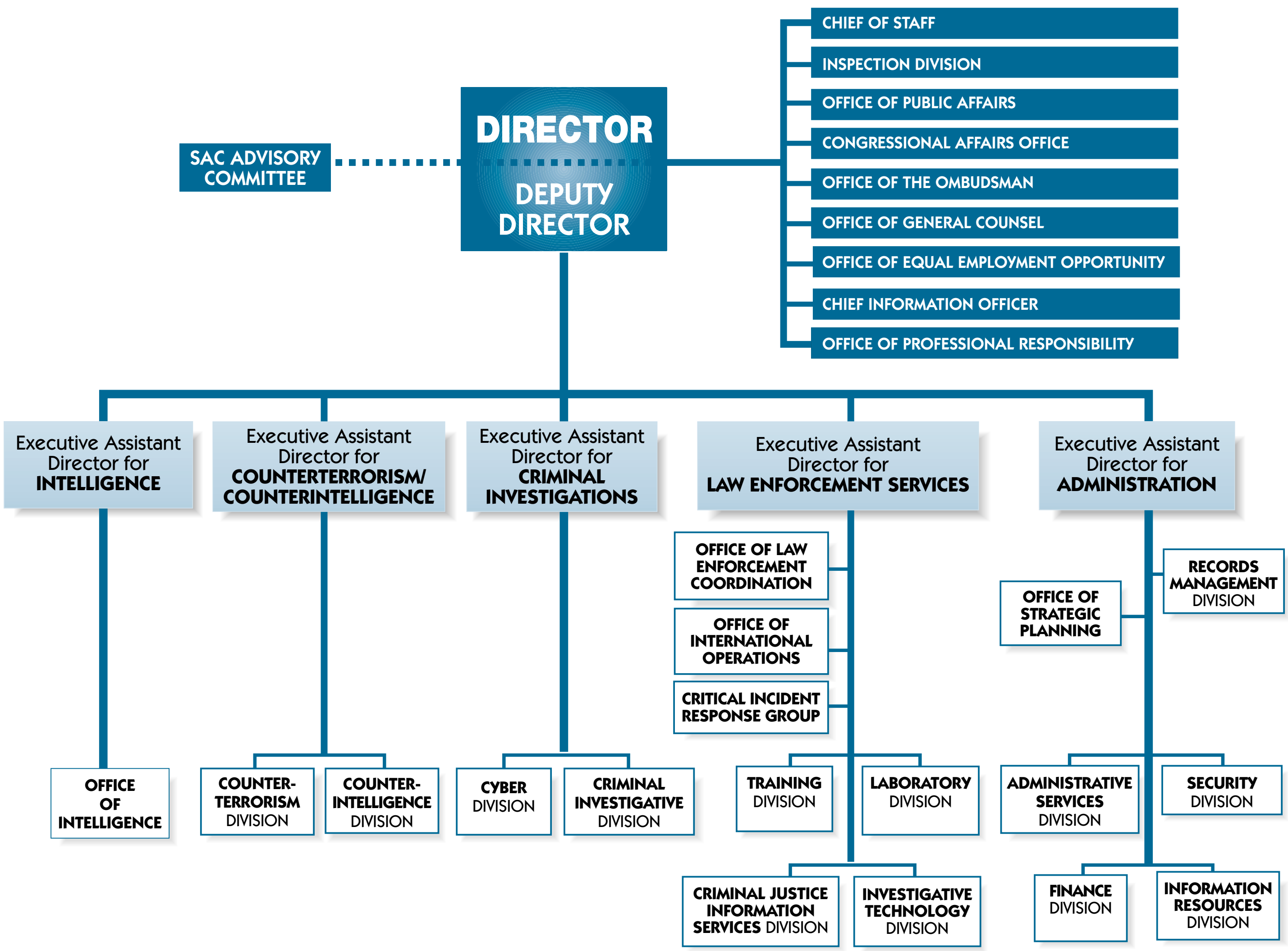
7 Administrative Reform

Re-engineering efforts are making our bureaucracy more efficient and more responsive to operational needs. We revised our approach to strategic planning, and we refocused our recruiting and hiring to attract individuals with skills critical to our counterterrorism and intelligence missions. We developed a more comprehensive training program and instituted new leadership initiatives to keep our workforce flexible. We are modernizing the storage and management of FBI records. We also built, and continue to improve, an extensive security program with centralized leadership, professional security personnel, more rigorous security measures, and improved security education and training.

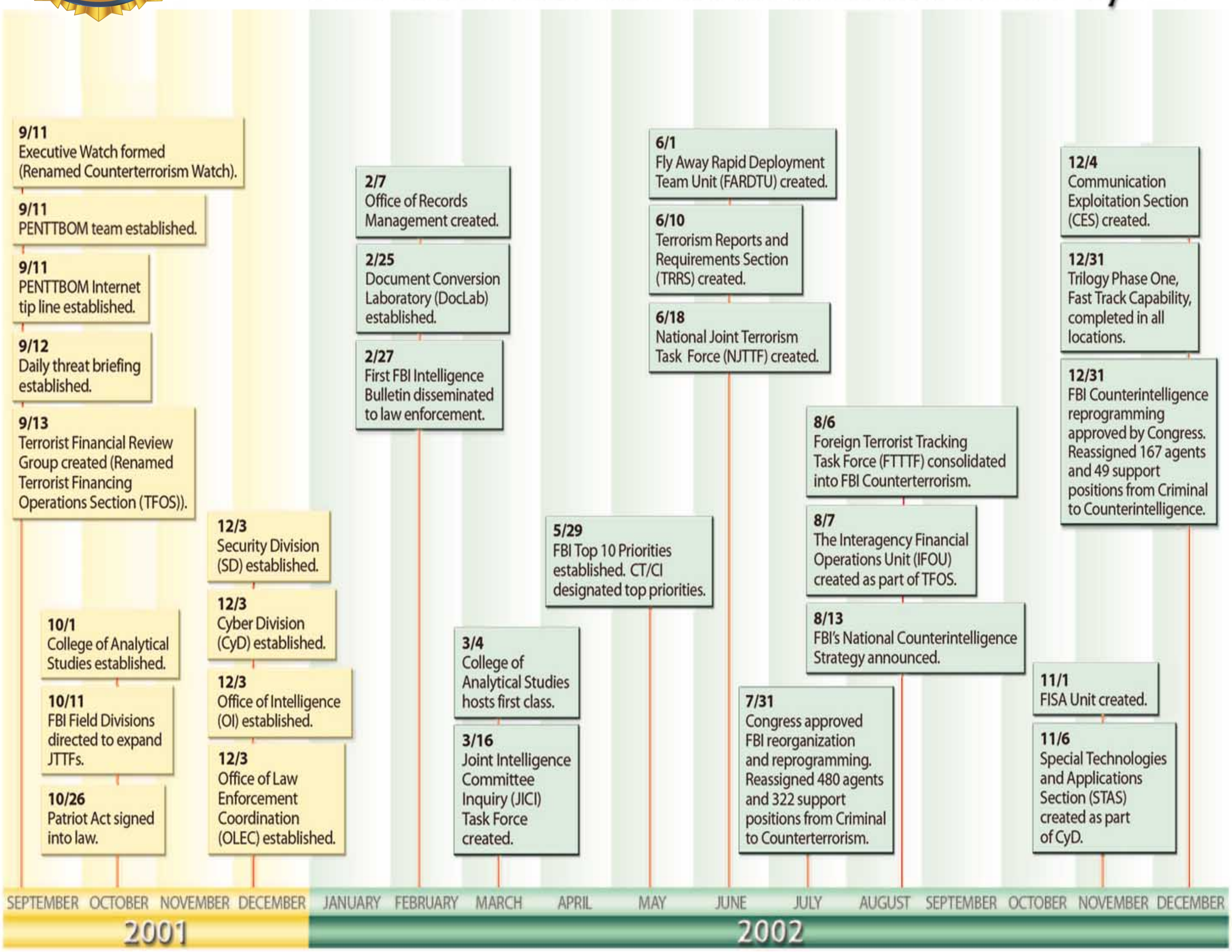
These improvements have produced tangible and measurable results. We significantly increased the number of human sources and the amount of surveillance coverage to support our counterterrorism efforts. We developed and refined a process for briefing daily threat information, and we considerably increased the number of FBI intelligence reports produced and disseminated. Perhaps most important, since September 11, 2001, we have participated in disrupting dozens of terrorist operations by developing actionable intelligence and better coordinating our counterterrorism efforts.

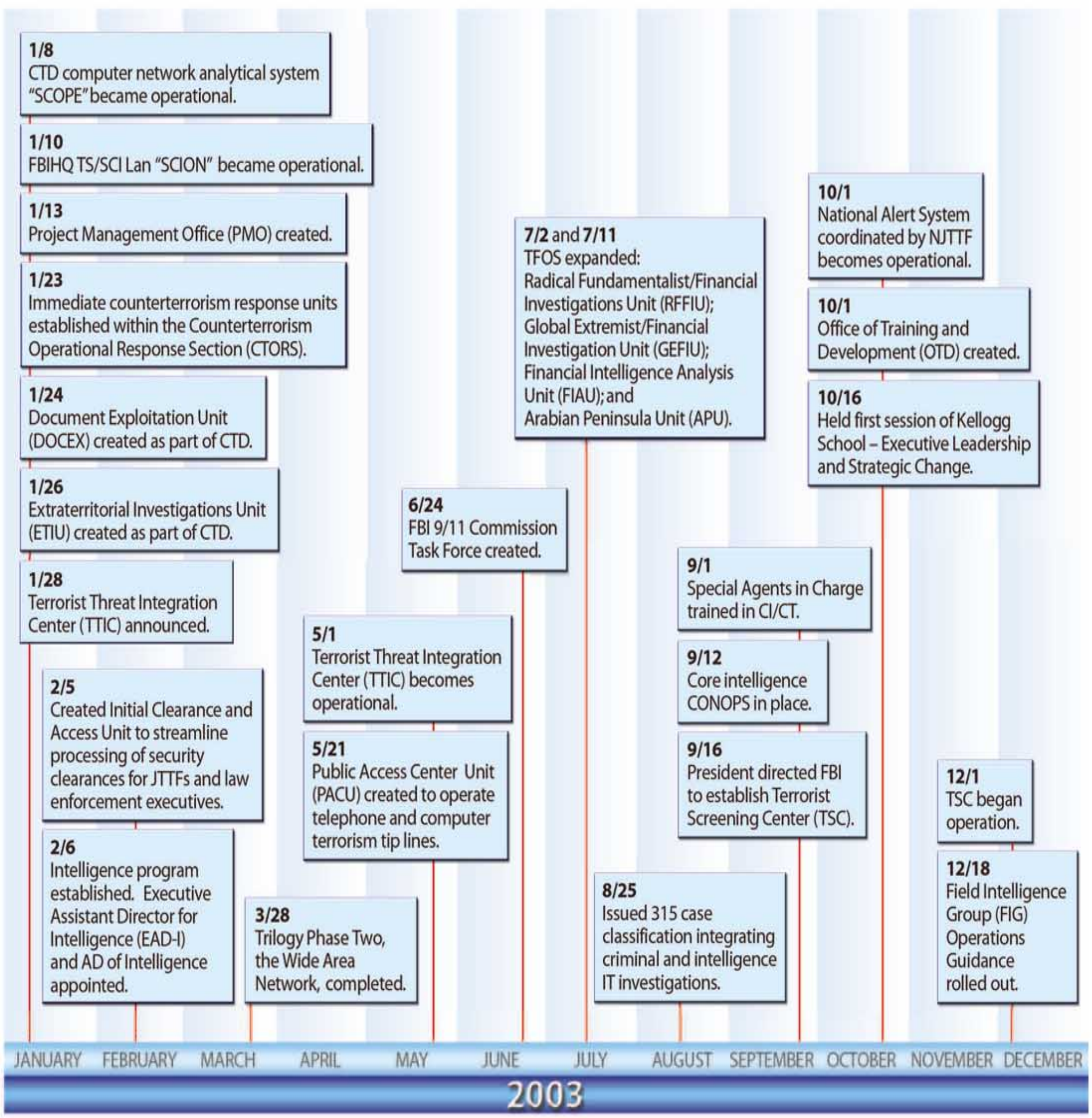
It is a testament to the character and dedication of the men and women of the FBI that they have implemented these reforms and realized this progress, while continuing to carry out their responsibility to investigate and protect America from criminal, counterintelligence, and terrorist threats of virtually unprecedented dimensions.

FEDERAL BUREAU OF INVESTIGATION



Enhancements to the FBI Counterterrorism Effort Post 9/11




1/8
CTD computer network analytical system "SCOPE" became operational.
1/10
FBIHQ TS/SCI Lan "SCION" became operational.
1/13
Project Management Office (PMO) created.
1/23
Immediate counterterrorism response units established within the Counterterrorism Operational Response Section (CTORS).
1/24
Document Exploitation Unit (DOCEX) created as part of CTD.
1/26
Extraterritorial Investigations Unit (ETIU) created as part of CTD.
1/28
Terrorist Threat Integration Center (TTIC) announced.
2/5
Created Initial Clearance and Access Unit to streamline processing of security clearances for JTTFs and law enforcement executives.
2/6
Intelligence program established. Executive Assistant Director for Intelligence (EAD-I) and AD of Intelligence appointed.
3/28
Trilogy Phase Two, the Wide Area Network, completed.
5/1
Terrorist Threat Integration Center (TTIC) becomes operational.
5/21
Public Access Center Unit (PACU) created to operate telephone and computer terrorism tip lines.
6/24
FBI 9/11 Commission Task Force created.
7/2 and 7/11
TFOS expanded:
Radical Fundamentalist/Financial Investigations Unit (RFFIU);
Global Extremist/Financial Investigation Unit (GEFIU);
Financial Intelligence Analysis Unit (FIAU); and
Arabian Peninsula Unit (APU).
8/25
Issued 315 case classification integrating criminal and intelligence IT investigations.
9/1
Special Agents in Charge trained in CI/CT.
9/12
Core intelligence CONOPS in place.
9/16
President directed FBI to establish Terrorist Screening Center (TSC).
10/1
National Alert System coordinated by NJTTF becomes operational.
10/1
Office of Training and Development (OTD) created.
10/16
Held first session of Kellogg School – Executive Leadership and Strategic Change.
12/1
TSC began operation.
12/18
Field Intelligence Group (FIG) Operations Guidance rolled out.
JANUARY
FEBRUARY
MARCH
APRIL
MAY
JUNE
JULY
AUGUST
SEPTEMBER
OCTOBER
NOVEMBER
DECEMBER
2003

INTRODUCTION

During the past 31 months, the FBI has undergone a transformation in all areas of its operations. The transformation has involved both the institution of new functions and capacities as well as refinements of existing processes and programs to modernize our operations. This report provides an overview of that reform process.

We have always had responsibility for the counterterrorism mission, and the Bureau has a history of impressive accomplishments in the war against terrorism. From the apprehension of Unabomber Theodore Kaczynski, to the investigation and prosecution of those responsible for the 1993 World Trade Center bombing, the 1995 Oklahoma City bombing, and the 1998 East Africa Embassy bombings, the FBI has investigated terrorist acts and helped to bring many of those responsible to justice. In addition, the Bureau has participated in preventing many terrorist acts before their commission, as evidenced by the foiling of the Millennium Plot to plant explosives at Los Angeles International Airport, the apprehension and prosecution of Ramzi Yousef and others for conspiracy to bomb United States commercial airliners, and the arrest and prosecution of Sheik Omar Abdel Rahman and his co-conspirators before they could carry out their plan to bomb office buildings, bridges, and tunnels in New York City.

Throughout his tenure, Director Louis Freeh and his executives took steps to build that preventive capacity within the Bureau. They established an Intelligence Section within the Investigative Services Division and staffed it with analysts who were tasked with identifying and predicting criminal and terrorist threats. They greatly enhanced our ability to coordinate investigations with our counterparts in other countries by nearly doubling the number of Legal Attaché offices overseas. Also, they devised and implemented a strategy for developing a counterterrorism capability in each FBI field office.

The FBI responded to the attacks of September 11, 2001, with a clear recognition that we needed both to build on the progress of the past decade and to enhance our operations and focus to meet the deadly challenge of modern terrorism. In a process that started on September 11, 2001, we have been reforming our organization, operations, and long-term objectives to make the prevention of terrorist attacks the Bureau's overriding priority.

This new operational focus required that we fundamentally transform our organization to enhance our ability to predict and prevent terrorism. We have followed a plan for this transformation that has seven basic elements:

- **Prioritization**
- **Mobilization**
- **Centralization**
- **Intelligence Integration**
- **Coordination**
- **Information Technology**
- **Administrative Reform**

These elements are the foundation of an effective Counterterrorism Program. The following describes each element of the plan in some detail.

PRIORITIZATION

In 1998, the FBI established a five-year strategic plan to set investigative priorities in line with a three-tiered structure. **Tier 1** included those crimes or intelligence matters – including terrorism – that threaten our national or economic security. **Tier 2** included offenses involving criminal enterprises, public corruption, and violations of civil rights. **Tier 3** included violations that affect individuals or property. This priority structure allowed supervisors substantial flexibility in applying the priorities to their decision making. Consequently, though a top-tier priority, the Counterterrorism Program did not receive a sufficiently significant increase in focus or resources.

On September 11, 2001, the prevention of further terrorism became the Bureau's dominant priority. On May 29, 2002, we formalized this prioritization by issuing a new hierarchy of programmatic priorities, with counterterrorism at the top. We developed these priorities by evaluating each criminal and national security threat within the Bureau's jurisdiction according to three factors: **1)** the significance of the threat to the security of the United States, as expressed by the President in National Security Presidential Directive 26; **2)** the priority the American public places on the threat; and **3)** the degree to which addressing the threat falls most exclusively within the FBI's jurisdiction.

The New Priorities

The FBI has ten top priorities. Priorities one through eight are program areas, and they are listed in the order in which they must be addressed. Priorities nine and ten are objectives that are key to the accomplishment of the programmatic priorities. The priorities are:

1 Protect the United States from Terrorist Attack

Every FBI manager, Special Agent, and support employee understands that the prevention of terrorist attacks is the FBI's overriding priority and that every terrorism-related lead must be addressed. Counterterrorism is the top priority in the allocation of funding, personnel, physical space, and resources, as well as in hiring and training. No matter their program assignment, all FBI field, operational, and support personnel stand ready to assist in our counterterrorism efforts.

2 Protect the United States Against Foreign Intelligence Operations and Espionage

The FBI is the lead federal agency with a mandate to investigate foreign counterintelligence threats within our borders. During the past 31 months, we have created a nationally-directed program for counterintelligence, staffed by a highly trained specialized workforce with enhanced analytical support, and with closer ties to the Intelligence Community. The program's focus is on: **1)** preventing hostile groups and countries from acquiring technology to produce weapons of mass destruction; **2)** preventing the compromise of personnel, information, technology, and economic interests vital to our national security; and **3)** producing intelligence on the plans and intentions of our adversaries.

3 Protect the United States Against Cyber-Based Attacks and High-Technology Crimes

We continue to see a dramatic rise in both cyber crimes, such as denial of service attacks, and traditional crimes that have migrated on-line, such as identity theft and child pornography. The FBI is the only government entity with the wide-ranging jurisdiction, technical resources, personnel, and network of relationships necessary to address the threat from multi-jurisdictional cyber crimes and cyber terrorism. Accordingly, the FBI created a national cyber program with a Cyber Division at FBI Headquarters and cyber squads in the field offices. The program focuses on identifying and pursuing: **1)** individuals or groups who conduct computer intrusions and spread malicious code; **2)** intellectual property thieves; **3)** Internet fraudsters; and **4)** on-line predators who sexually exploit or endanger children.

4 Combat Public Corruption at All Levels

The FBI has extensive experience investigating public corruption. Our public corruption investigations focus on all levels of government *(local, state, and federal)* and address all types of judicial, legislative, regulatory, and law enforcement corruption.

5 Protect Civil Rights

The FBI is the federal agency with responsibility for investigating allegations of federal civil rights violations and abuses. In pursuit of this mission, the FBI investigates allegations of brutality and related misconduct by law enforcement officers as well as hate crimes. Recently, our civil rights program has focused particularly on hate crime cases related to Muslim, Sikh, and Arab-American communities that suffered threats and attacks in the aftermath of September 11, 2001, and Operation Iraqi Freedom.

6 Combat Transnational and National Criminal Organizations and Enterprises

As the world grows smaller and investigations become more international, the FBI increasingly uses its expertise and relationships with foreign counterparts to dismantle or disrupt those major criminal enterprises that are responsible for cross-border criminal activity.

7 Combat Major White-Collar Crime

The FBI has expertise in the investigation of white-collar criminal activities that are international, national, or regional in scope. During the past two years, we have dedicated scores of agents to the investigation of corporate scandals involving Enron, WorldCom, and others, and focused our criminal analytical capabilities on major health care fraud and bank fraud threats. At the same time, we are scaling back our investigations into smaller bank frauds and embezzlements that are ably handled by other agencies and our state and municipal partners.

8 Combat Significant Violent Crime

Most violent crime in the U.S. is investigated and prosecuted by state or municipal authorities. While federal statutes give the FBI jurisdiction over many types of violent crime, we choose our investigations carefully so as not to duplicate the tremendous job being done by our state and municipal partners. We concentrate our efforts on those criminal targets – such as organized criminal enterprises and violent narcotics gangs – that pose a significant threat to our society. We participate in the fight against violent crime wherever we bring something special to the mix, whether it is special capabilities, resources, or our jurisdiction to enforce applicable federal statutes.

9 Support Federal, State, Municipal, and International Partners

Our preventive mission requires a high level of engagement with state and municipal law enforcement, other federal agencies, members of the Intelligence Community, and our international counterparts. Accordingly, we have made it a top priority to improve information sharing and coordination, and to provide training and other support to our partners.

10 Upgrade Technology to Successfully Perform the FBI's Mission

We are upgrading our technology by deploying a state-of-the-art secure network, putting new computers with new software on desktops, and building centralized databases. We are expanding our capabilities to fully exploit digital information and to share the results internally and externally. We also are educating our workforce to ensure that everyone understands how technology can help us do our job better.

Implementing the New Priorities

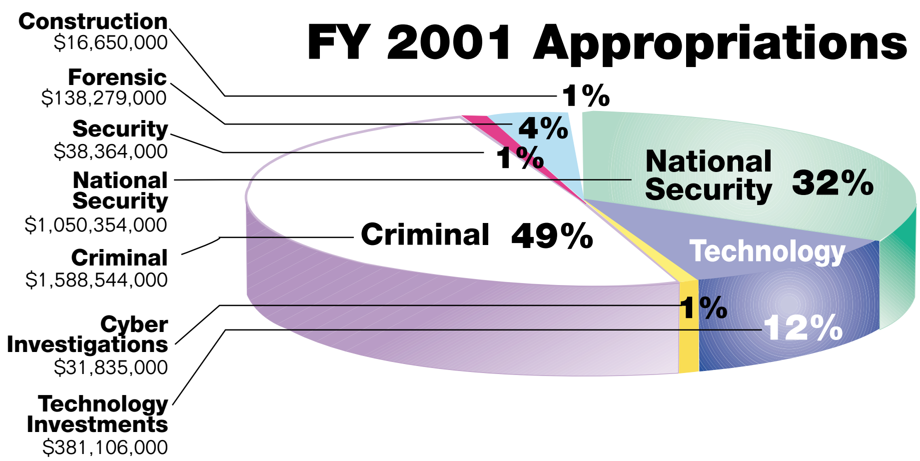
To ensure adherence to the new priorities, we reduced the flexibility that was built into the old three-tiered system. Instead of allowing field offices to choose how to allocate resources within broad priority areas, the new system dictates that managers satisfy operational needs in the strict order of their priority. Special Agents in Charge *(SACs)* making deployment decisions must first dedicate sufficient resources to handle priority one before handling priority two, and so forth. Similarly, Headquarters managers must provide services – such as training, hiring, and technology improvements – to operational programs in order of priority.

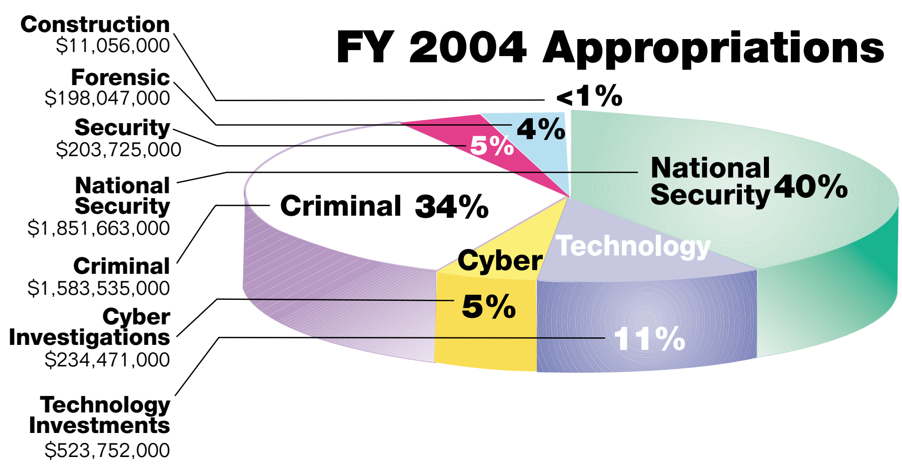
Communication of Priorities

Understanding that successful implementation of the new priorities requires universal commitment to them, we embarked on a multi-faceted education campaign. We significantly increased the number of SAC conferences where we discuss the new priorities and task the SACs to communicate the message to their personnel in the field. Senior Headquarters executives regularly discuss the priorities in speeches, congressional testimony, published articles, employee e-mails and meetings. The FBI's intranet and employee publications, such as *The Investigator* magazine, provide continued updates and guidance on the new priorities to our employees. Also, a number of senior executives have begun traveling to each field office to deliver a multimedia presentation that educates employees about the current status of our new priorities and associated organizational reforms.

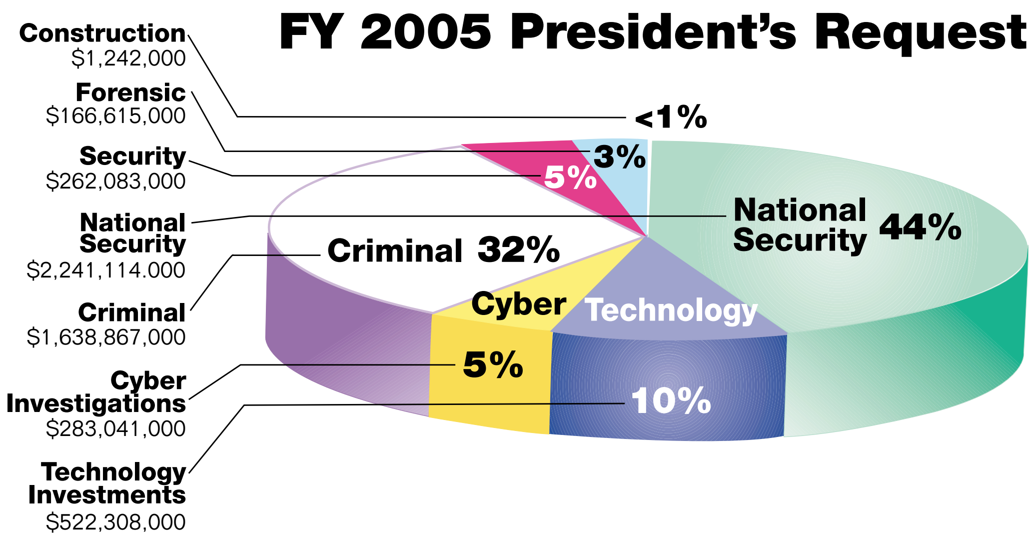
Priorities in the Budgetary Process

Our commitment to these priorities is reflected in our budget and resource management. Counterterrorism and intelligence-related funding and personnel needs have been the top priorities in our budget requests to the Attorney General, the President, and the Congress since the events of September 11, 2001. In Fiscal Year *(FY)* 2001, approximately 32 percent of the FBI's annual appropriation was dedicated to national security programs *(counterterrorism and counterintelligence)*. For FY 2004, that number is 40 percent of the overall budget.





For FY 2005, the President has submitted a budget proposal that calls for further increases in the resources available for counterterrorism activities and expands the percentage of the FBI's budget dedicated to national security matters to 44 percent. Compared to FY 2001, this more than doubles the amount of funding for counterterrorism and counterintelligence and equates to an 80 percent increase in the number of people devoted to the counterterrorism and counterintelligence missions.



Enforcement of Priorities

Senior managers at Headquarters and in the field have been instructed that they must address and resolve every counterterrorism lead, even if it requires a diversion of personnel or resources from other priority areas. On two occasions, Headquarters received indications that a field office's operations appeared inconsistent with this directive. Inspectors were sent to these field offices to conduct a thorough audit and to determine whether the office was complying with the new priorities. In the one instance where a problem was found, inspectors made recommendations for correcting the problem, and these recommendations were promptly implemented.

We are revising our performance metrics and inspection criteria to better evaluate performance and resource allocation in accordance with the new priorities. These measures are discussed in more detail under Intelligence Integration *(page 34)*.

Mobilization

In accordance with the new priorities, we mobilized and substantially reallocated resources and personnel to the counterterrorism mission. We increased the number of counterterrorism agents, intelligence analysts, and translators, and established a number of new operational components dedicated to the counterterrorism mission. Each of these components represents a new capacity, or an enhanced capacity, for the Bureau in the war against terrorism. In addition, FBI personnel who do not work on counterterrorism matters full-time stand by to support our number one priority as needed.

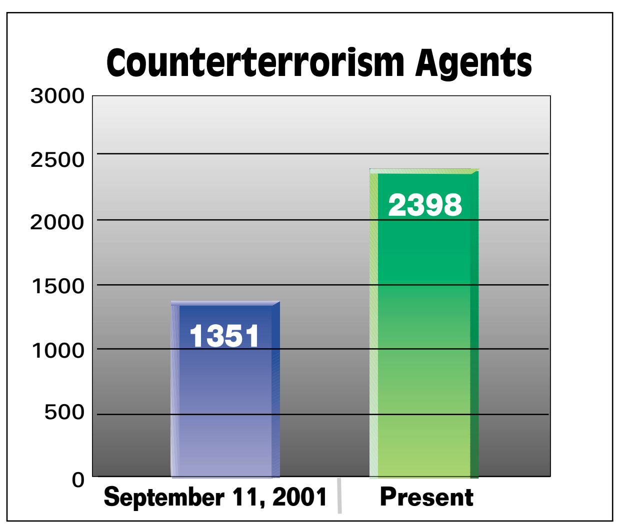
As of February 29, 2004, the FBI has just over 28,000 employees, of which 11,881 are Special Agents. These men and women provide a surge capacity that enables the FBI to respond to terrorism threats and to ensure that every terrorism lead is followed to its resolution. In the autumn of 2001, approximately 67 percent, or more than 4,000 of our agents in the field who previously worked on criminal investigative matters were diverted to investigate the September 11, 2001, attacks or the subsequent anthrax attacks. Analysts from the Counterintelligence and Criminal Investigative Divisions also were deployed to assist in these counterterrorism efforts.

Today, all Special Agents are adept in the use of the investigative tools used in counterterrorism investigations and can be mobilized to assist counterterrorism efforts when needed. The fact that counterterrorism is the top priority for the Criminal Investigative Division ensures that all of its personnel will be made available when this surge capacity is required. Standardized processes for conducting analysis and producing intelligence products allow for all FBI analysts to lend assistance to the Counterterrorism Program. The flexibility to leverage and mobilize all our personnel in this manner is critical to our ability to respond quickly to evolving threats.

Personnel Mobilized

Special Agents

Since September 11, 2001, we have increased the number of Special Agents working terrorism matters from 1,351 to 2,398.



Intelligence Analysts

We have increased the number of analysts supporting our counterterrorism mission. Immediately after September 11, 2001, we transferred analysts from other divisions to counterterrorism and integrated analysts detailed from other agencies – including 25 analysts and an analyst supervisor detailed from the Central Intelligence Agency *(CIA)*. Since then, we have made progress toward building a strong analytical cadre through targeted recruitment and enhanced training and career development.

FBI ANALYSTS

YEAR	TOTAL	HIRED
FY 2001	1023	42
FY 2002	1012	96
FY 2003	1180	250
3/4/2004	1197	72
	Grand Total	460

Translators

Our Counterterrorism Program relies heavily on linguistic capabilities for translation services, interview support, and surveillance activities, and these needs are growing. Since September 11, 2001, electronic surveillance collection in Arabic, Urdu, Pashto, and various other Middle Eastern languages has increased by 75 percent or more. To meet this growing need, since the beginning of FY 2001, we have recruited and processed more than 30,000 translator applicants. These efforts have resulted in the addition of nearly 700 new translators, including both FBI employees and contract linguists.

More than 95 percent of our translators are native speakers of the foreign language. Their native proficiencies equip them with both a firm grasp of colloquial and idiomatic speech, and an understanding of the religious, cultural, and historical references needed to effectively perform the wide range of services required of an FBI linguist. To further ensure the quality of translations, on December 1, 2003, we instituted a national quality control program. All material produced by translators on board for less than three months is subject to accuracy and content reviews by senior staff, and their products are subject to periodic audits thereafter. Our translator corps is complemented by well over 1,000 Special Agents and intelligence analysts with foreign language proficiencies at the minimum working level or higher.

INCREASED LANGUAGE TRANSLATION CAPABILITIES
to Support Counterterrorism

MAJOR LANGUAGE	9/11/01	Present	Net Change
Arabic	70	207	+137
Farsi	24	55	+31
Pashto	1	10	+9
Urdu	6	21	+15
Chinese	67	119	+52
French	16	34	+18
Hebrew	4	11	+7
Korean	18	25	+7
Kurdish	0	5	+5
Russian	78	100	+22
Turkish	2	10	+8

Expanded Operational Capabilities

Counterterrorism Watch

On September 11, 2001, we formed the Executive Watch, later renamed the Counterterrorism Watch Unit *(CT Watch)*. CT Watch receives threat information from a variety of sources, including FBI Headquarters divisions, field offices, Joint Terrorism Task Forces *(JTTFs)*, the intelligence and homeland security communities, and state and municipal law enforcement. CT Watch assesses information for credibility and urgency, and tasks appropriate FBI divisions to take action on or further investigate that information.

National Joint Terrorism Task Force

Immediately following the attacks of September 11, 2001, an *ad hoc* group of representatives from federal agencies began meeting, sharing information, and working together in the FBI's Strategic Information Operations Center *(SIOC)* at Headquarters. On July 18, 2002, we formally created the National Joint Terrorism Task Force *(NJTTF)* to act as a liaison and conduit for information on threats and leads from FBI Headquarters to the local JTTFs and to 38 participating agencies. The NJTTF now includes representatives from members of the Intelligence Community; components of the Departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and the Interior; the City of New York Police Department; the Nuclear Regulatory Commission; Railroad Police; U.S. Capitol Police; and others.

All members are provided with access to the FBI intranet, including its internal e-mail system, and to the FBI's investigative database for purposes of counterterrorism investigations. In turn, members provide access to their organizations' respective databases. In addition, Daily Secure Video Conferences, coordinated by the National Security Council, are held within SIOC and attended by NJTTF members, ensuring that all member agencies of the NJTTF receive the latest threat briefings.

The NJTTF also works with the FBI's Office of Intelligence to coordinate inter-agency intelligence-gathering initiatives, such as the following:

Foreign Flight Crew Vetting

In September 2003, the Department of Homeland Security *(DHS)* requested assistance in vetting certain foreign flight crew members who have access to commercial aircraft cockpits while in U.S. airspace. The Transportation Security Administration *(TSA)* provided 6,200 names and dates of birth to the National Joint Terrorism Task Force. The NJTTF ran the names against a number of FBI and Intelligence Community databases and identified 184 possible matches. The NJTTF then assembled members from several federal agencies to review the findings and to determine if any possible matches posed a threat to aviation using the TSA's baseline for a "No Fly List" candidate. After a thorough review, 25 names were placed on the "No Fly" list.

Maritime Initiatives

The NJTTF is spearheading the Maritime Threat Project – a multi-agency, cooperative effort to prevent or disrupt potential maritime attacks. The Maritime Threat Project consolidates information on suspicious activities – such as persons conducting surveillance around ports – and forwards appropriate leads to local JTTFs and other agencies for additional investigation. As a part of this Maritime Threat Project, for example, the NJTTF sent leads to all JTTFs with instructions for them to canvass diving schools in their areas to identify suspicious activity and potential leads.

A related effort is "Operation Drydock," in which the Coast Guard Investigative Service and the NJTTF collaborated to identify and appropriately respond to national security concerns related to merchant marine documents and licenses. This initiative addresses the use of fraudulent credentials by individuals seeking to work aboard commercial ships, and recently identified 11 individuals with ties to terrorist organizations.

Operation TRIPWIRE

Operation TRIPWIRE is designed to improve the FBI's intelligence base with a specific goal to aid in identifying potential terrorist sleeper cells within the U.S. It puts in place a roadmap for developing intelligence and collection requirements targeting terrorist training, financing, recruiting, logistical support, and pre-attack preparation within the U.S.

Examples of TRIPWIRE operations are as follows:

Agricultural Aviation Threat Project

The FBI, through the NJTTF, identified and interviewed agricultural aviation owners and operators throughout the country. The FBI reviewed a list of over 11,000 aircraft provided by the Federal Aviation Administration *(FAA)*, and interviewed 3,028 crop duster owners and operators. To date, this effort has led to the initiation of several counterterrorism investigations.

Correctional Intelligence Initiative

Another initiative being coordinated through the NJTTF aims to detect and interdict efforts by al-Qa'ida and other terrorist groups to recruit within the U.S. prison inmate population. All JTTFs have been tasked to coordinate with the correctional agencies within their respective geographic regions to exchange intelligence and recruit human sources. JTTF members are identifying existing or former sources who are now incarcerated and reactivating them to infiltrate any radical elements. To date, these efforts have identified approximately 370 connections between particular inmates and domestic and international terrorism investigations, and have identified a number of instances of potential terrorism-related activity within the prisons.

Terrorism Financing Operations Section

On September 13, 2001, we created the Financial Review Group, later renamed the Terrorism Financing Operations Section *(TFOS)*, to consolidate our approach to dismantling terrorist financing operations. TFOS works not only to identify and track financial transactions and links after a terrorist act has occurred; it exploits financial information to identify previously unknown terrorist cells, to recognize potential terrorist activity or planning, and to predict and prevent potential terrorist acts.

TFOS is both an operational and coordinating entity. Operationally, TFOS has been involved in the financial investigations of more than 3,000 individuals and groups suspected of financially supporting terrorist organizations, and joint efforts with its partners have resulted in the blocking or freezing of millions of dollars in assets. TFOS works closely with our experts in criminal money laundering, and leverages the resources of our Financial Crimes Section in the Criminal Investigative Division as needed.

As a coordinating entity, TFOS ensures that a unified approach is pursued in investigating terrorist financing networks. TFOS coordinates financial aspects of FBI terrorism investigations, establishes overall initiatives and policies on terrorist financing matters, and coordinates with the National Security Council's Policy Coordinating Committee on Terrorist Financing, the Department of Justice *(DOJ)*, and the financial services sector. Also, terrorist finance coordinators participate in every JTTF. Through TFOS, the FBI has succeeded in building strong working relationships with all law enforcement and intelligence agencies that are fighting the war on terror.

Evidence Exploitation

Prior to September 11, 2001, the FBI and its partners lacked sufficient procedures for systematically exploiting paper documents, electronic media, and forensic evidence for its intelligence value. The National Media Exploitation Center was established in late 2001 to coordinate FBI, CIA, the Defense Intelligence Agency *(DIA),* and National Security Agency *(NSA)* efforts to analyze and disseminate information gleaned from millions of pages of paper documents, electronic media, videotapes, audiotapes, and electronic equipment seized by the U.S. military and Intelligence Community in Afghanistan and other foreign lands. These exploitation efforts have produced approximately 20,000 investigative leads, and forensic evidence such as fingerprints and DNA from documents and items recovered from suspects overseas have proven critical to a number of terrorist apprehensions and disruptions.

We have since established groups that specialize in the analysis of particular types of information. On December 4, 2002, we created a Communications Exploitation Section to coordinate the analysis of documents, electronic media, and forensic evidence, as well as telephone and electronic communications. Soon thereafter, we established a specialized Document Exploitation Unit to exploit terrorist-related documentary material and to extract threat and intelligence information for the FBI and the Intelligence Community. In December 2003, we began preliminary operations at the Terrorist Explosive Device Analytical Center at the FBI Laboratory in Quantico, Virginia. This new center, described in more detail on page 45, coordinates the efforts of multiple federal agencies to collect, analyze, forensically exploit, and disseminate intelligence related to improvised explosive devices.

Fly-Away/Rapid Deployment Teams

On June 6, 2002, the FBI created the Fly Away/Rapid Deployment Team Unit to manage and support the field office-based Rapid Deployment Teams and the newly created Headquarters-based "Fly Squads." These specialized teams and squads lend counterterrorism knowledge and experience, language capabilities, and intelligence analysis support to FBI field offices and Legal Attachés whenever they are needed. Since September 11, 2001, the Headquarters-based Fly Squads have been deployed on 38 different occasions, and have assisted in operations from Buffalo, New York, to the Gaza Strip.

Foreign Terrorist Tracking Task Force

On October 29, 2001, President Bush issued Homeland Security Presidential Directive No. 2, directing the Attorney General to create the Foreign Terrorist Tracking Task Force *(FTTTF)* to keep foreign terrorists and their supporters out of the U.S. through entry denial, removal, or prosecution. FTTTF participants include the FBI, CIA, and the Departments of Homeland Security, Treasury, State, and Energy. The FTTTF also maintains a close liaison with intelligence and law enforcement services in Canada, Australia, the United Kingdom, and other countries. On August 6, 2002, the Attorney General directed the consolidation of the FTTTF into the FBI.

To fulfill its mission, the FTTTF implemented information sharing agreements among participating agencies to assist it in locating suspected terrorists and their supporters. It now has access to over 40 sources of data containing lists of known and suspected foreign terrorists and their supporters, including the FBI's Violent Gang and Terrorist Offenders File *(VGTOF)* and the State Department's TIPOFF watch list.

Relying on this base of information, the FTTTF performs two primary analytical functions:

Tracking and Detection The FTTTF analyzes immigration records, other law enforcement data, and public and proprietary source information to detect the presence of terrorists in the U.S. This service supports the activities of JTTFs and other counterterrorism investigators by helping identify the current and previous locations of suspected terrorists in the U.S. To date, this process has generated more than 200 leads to the potential location of terrorists.

Risk Assessment The FTTTF uses human analysis and analytical software to assess the risk of specific categories of foreign nationals attempting to enter the U.S. In compliance with the Aviation Transportation and Security Act, the FTTTF also conducts background records checks and risk assessments on foreign nationals seeking flight training on aircraft weighing 12,500 pounds or more. As of December 2003, the FTTTF has done more than 58,000 such checks. In accordance with the Century of Aviation Reauthorization Act, passed on December 12, 2003, we will soon be transferring this function to the DHS's Transportation Security Administration.

Bioterrorism Risk Assessment Group

Pursuant to the Public Health Security and Bioterrorism Preparedness Act of 2002, the FBI's Criminal Justice Information Services Division *(CJIS)* now conducts background checks and risk assessments on individuals who have or seek access to specific biological agents and toxins. To meet this new mandate, CJIS established procedures for completing the assessments, set up a database for tracking the assessments, and reassigned and hired additional personnel. As of January 26, 2004, assessments were finalized for 7,848 individuals, and 41 were determined to be "restricted persons" as defined by the Bioterrorism Preparedness Act. "Restricted persons" cannot be allowed by the employing lab to possess, use, transport, or have access to select agents or toxins.

Foreign Intelligence Surveillance Act Unit

In November 2002, we created a specialized unit within the Office of General Counsel to support and streamline functions related to the Foreign Intelligence Surveillance Act *(FISA)* process. The new unit coordinates with FBI field offices, FBI Headquarters, and DOJ to ensure that FISA packages are prepared and reviewed in an expeditious and consistent manner. The FISA Unit, in coordination with other appropriate Headquarters personnel, is overseeing the development and implementation of the new FISA management system that will enable us both to transmit a FISA document between field offices, the operational units at FBI Headquarters, the Office of General Counsel's National Security Law Branch, and DOJ's Office of Intelligence Policy and Review, and to track its progress during each stage of the review and approval process. An automated tracking system will identify delays and chokepoints in the process, and the FISA Unit will remedy identified problems by sending reminders or resolving outstanding questions.

Language Translation

Connecting Translation Capabilities

The FBI's approximately 1,200 translators are stationed across 52 field offices and Headquarters, and are now connected via secure networks that allow a translator in one

FBI office to work on projects for any other office. We implemented network enhancements to ensure that collected intelligence can be transmitted to the appropriate translator on a near real-time basis, and we developed work flow management software to track, monitor, and account for any collected data and the corresponding translation product.

Language Services Translation Center

Shortly after September 11, 2001, we established the Language Services Translation Center *(LSTC)* at FBI Headquarters to help ensure that translation services are available whenever and wherever they are needed. The LSTC acts as a “command and control” center to coordinate translator assignments, and to ensure that our translator resources are aligned strategically with operational and intelligence priorities. In addition, the LSTC has an on-site population of 20 FBI translators and 29 contract translators who render immediate translation assistance to field offices and Legal Attaché offices when required.

National Virtual Translation Center

To provide similar capabilities to the larger Intelligence Community, in accordance with Section 907 of the USA PATRIOT Act, the Director of Central Intelligence established the National Virtual Translation Center *(NVTC)* on February 11, 2003, and designated the FBI as its Executive Agent. Like the FBI’s LSTC, the NVTC serves as a clearinghouse to provide timely and accurate translation of foreign intelligence for Intelligence Community agencies. The NVTC taps into the FBI’s pool of contract linguists and matches excess translation capacity with the translation needs of other Intelligence Community agencies. The FBI further supports the NVTC by handling recruiting and applicant processing for NVTC linguists.

Although it will not be fully “virtual” until later this spring, the NVTC has already successfully completed translation tasks for CIA, DIA, and the FBI. With its Director from NSA, and its Deputy Directors from CIA and the FBI, the NVTC is truly a Community-wide effort.

Special Technologies and Applications Section

In November 2002, we created a Special Technologies and Applications Section within the new Cyber Division to support counterterrorism, counterintelligence, and criminal investigations involving computer intrusions and digital or electronic media evidence. The Section provides technical investigative analysis, helping to extract and decrypt volumes of data and making it easily searchable by investigators and intelligence analysts. The Section also designs automated tools, acts as a clearinghouse for new technologies developed by other agencies and the private sector, and coordinates with research and development entities inside and outside government. These efforts help ensure that the FBI is prepared to fully exploit digital evidence for its intelligence value and to respond to new computer intrusion-related threats and incidents.

Investigative Technology Division

Recognizing that the effective and focused use of applied science and engineering resources is critical to our efforts, especially our efforts to protect the U.S. from a terrorist attack, we created the Investigative Technology Division *(ITD*) out of components of the Laboratory Division in August 2002. The mission of ITD is to develop and provide state-of-the-art technical support and expertise to enhance the FBI's investigative efforts. ITD also oversees forensic services related to the collection and processing of computer, audio, and visual media to ensure such evidence is fully exploited for its intelligence value.

The ITD develops, procures, and supports technologies which are broadly applicable to all FBI investigative programs within ITD's designated technology program areas *(namely, Electronic Surveillance, Physical Surveillance, Digital Forensics, Surreptitious Entry, Tactical Communications, and Defensive Programs).*

The refocusing of the FBI's efforts to proactively address terrorism and foreign intelligence threats has resulted in a 64 percent increase in, and a substantial realignment of, ITD's workload. This chart depicts the alignment of the tactical workload of ITD entities in FY 1996 *(historical)* and FY 2003 *(current).*

DISTRIBUTION of TACTICAL WORKLOAD

Fiscal Year	FY 1996	FY 2003
Criminal Investigations	48%	15%
Counter-intelligence	42%	42%
Counter-terrorism	10%	43%
Grand Total	100%	100%

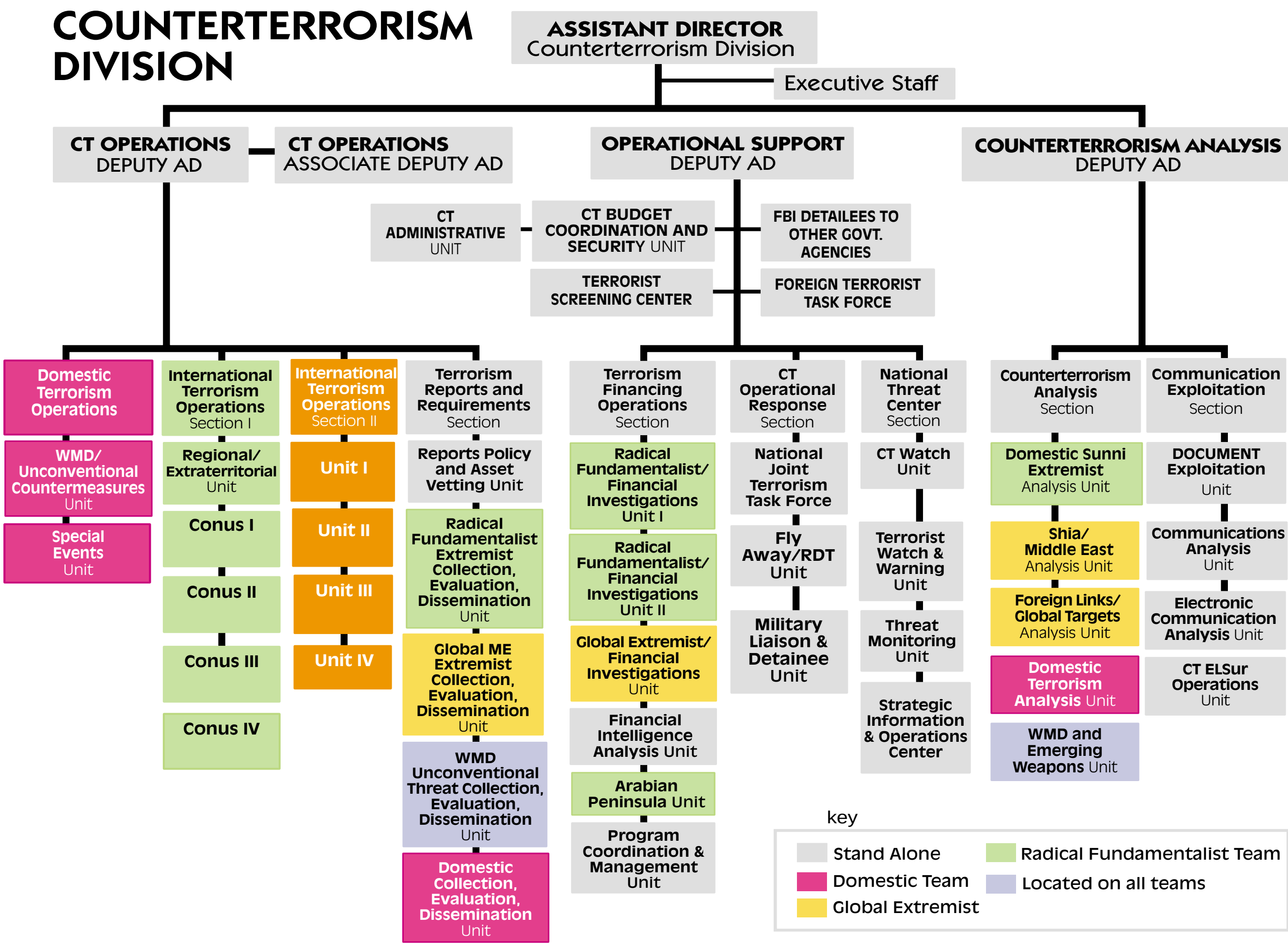
CENTRALIZATION

Prior to September 11, 2001, the Bureau had no centralized structure for the national management of its Counterterrorism Program, and terrorism cases were routinely managed out of individual field offices. An al-Qa'ida case, for example, might have been run out of the New York Field Office; a HAMAS case might have been managed by the Washington Field Office. This arrangement functioned for years, and produced a number of impressive prosecutions.

Once counterterrorism became our overriding priority, however, it became clear that this arrangement had a number of failings. It "stove-piped" investigative intelligence information among field offices. It diffused responsibility and accountability between counterterrorism officials at FBI Headquarters and the SACs who had primary responsibility for the individual terrorism investigations. It allowed for field offices to assign varying priorities and resource levels to terrorist groups and threats. It impeded oversight by FBI leadership, and it complicated coordination with other federal agencies and entities involved in the war against terrorism. For all these reasons, we decided that the Counterterrorism Program needed centralized leadership.

In December 2001, we reorganized and expanded the Counterterrorism Division *(CTD)* at Headquarters and created the position of Executive Assistant Director *(EAD)* for Counterterrorism and Counterintelligence. *(The Assistant Director of CTD reports to the EAD.)* We now have the centralized management to run a truly national program – to coordinate counterterrorism operations and intelligence production domestically and overseas; to conduct liaison with other agencies and governments; and to establish clear lines of accountability for the overall development and success of our Counterterrorism Program. With this management structure in place, we are driving the fundamental changes that are necessary to accomplish our counterterrorism mission.

We divided the operations of the Counterterrorism Division into branches, sections, and units, each of which focuses on a different aspect of the current terrorism threat facing the U.S. These components are staffed with intelligence analysts and subject matter experts who work closely with investigators in the field and integrate intelligence across component lines. This integration allows for real-time responses to threat information and quick communication with decision-makers and investigators in the field.



Investigative Operations Branch

The Investigative Operations Branch supports, coordinates, and manages terrorism-related investigations. It is comprised of four sections.

The International Terrorism Operations Section I (ITOS I)

ITOS I supports, coordinates, and provides oversight of FBI international counterterrorism operations related to al-Qa'ida and other Sunni extremist groups.

The International Terrorism Operations Section II (ITOS II)

ITOS II supports, coordinates, and provides oversight of FBI international counterterrorism operations related to other groups, such as Hizballah, HAMAS, and Palestinian Islamic Jihad, as well as the terrorist threat from state sponsors of terrorism.

The Domestic Terrorism Operations Section (DTOS)

DTOS supports, coordinates, and provides oversight of FBI domestic counterterrorism operations. In addition, DTOS's Special Events Unit plays a major role in planning, coordinating, and managing support to field offices charged with counterterrorism responsibilities for special events such as the Super Bowl or Olympic Games.

The Terrorism Reports and Requirements Section

The Terrorism Reports and Requirements Section oversees the dissemination of raw intelligence reports and executes policies and procedures established by the Office of Intelligence.

Operational Support Branch

The Operational Support Branch handles administrative responsibilities for CTD, and administers the Foreign Terrorist Tracking Task Force, the Terrorist Screening Center, and the Terrorist Financing Operations Section *(all of which are described in detail elsewhere in this report)*. This branch also runs two critical components of our counterterrorism operations.

National Threat Center Section

The National Threat Center Section administers CT Watch and other units related to threat management: **1)** the Public Access Center Unit that receives threat information from the public and forwards it to the appropriate unit; **2)** the Terrorist Watch and Warning Unit that produces finished intelligence products for the law enforcement community *(such as Intelligence Bulletins and Special Event Threat Assessments)*; and **3)** the Threat Monitoring Unit that collects threat information, looks for patterns and connections, and provides "raw" threat-related intelligence reports. This Section also runs SIOC, the 24/7 command and crisis response center at FBI Headquarters.

Counterterrorism Operational Response Section

The Counterterrorism Operational Response Section lends critical support in three areas. It supports the National Joint Terrorism Task Force; it coordinates deployment of the Headquarters-based "Fly Teams" and the field office-based Rapid Deployment Teams; and it conducts liaison with the Department of Defense *(DOD)* and manages FBI personnel working with the military in Guantanamo Bay, Cuba, and Afghanistan.

Counterterrorism Analysis Branch

The Counterterrorism Analysis Branch oversees the bulk of the CTD's intelligence functions, including analysis, evidence exploitation, and the preparation and dissemination of finished intelligence products and briefing materials. Today, the Counterterrorism Analysis Branch operates with the guidance and oversight of the FBI's Office of Intelligence and is a vital part of the FBI's enterprise-wide intelligence program. It is comprised of two sections.

Counterterrorism Analysis Section

The Counterterrorism Analysis Section includes five units whose areas of focus mirror those of the units in the Investigative Operations Section. These units examine the composition, activities, tradecraft, ideology, and linkages of terrorist groups, and they assess terrorist activities and threats to assist FBI managers in making decisions about deployments and the allocation of resources.

Communications Exploitation Section

The Communications Exploitation Section processes information and disseminates information derived from the full range of media. It is an integral participant in the National Document Exploitation Center process.

INTELLIGENCE INTEGRATION

The Bureau is designed, and has always operated, as both a law enforcement and an intelligence agency. It has the dual mission: **1)** to investigate and arrest perpetrators of completed crimes *(the law enforcement mission)*; and **2)** to collect intelligence that will help prevent future crimes and assist policy makers in their decision making *(the intelligence mission)*. History has shown that we are most effective in protecting the U.S. when we perform these two missions in tandem.

Agents long ago recognized that investigations could produce intelligence benefits beyond arrest and prosecution. Starting with the Ku Klux Klan cases in the 1960's and the Mafia cases of the 1970's, our agents began to view criminal investigations not only as a means of arresting and prosecuting someone for a completed crime, but also as a means of obtaining information to prevent future crime. Their goal was not simply to arrest individual members of the Klan or the Mafia, but to penetrate and dismantle the whole criminal organization.

As agents adopted this approach, they further developed the intelligence tools – such as electronic surveillance and the cultivation of human sources – that are critical to predicting and preventing criminal activity. They also learned to think strategically before making arrests, sometimes opting to delay a suspect's arrest to allow more opportunity for surveillance that might disclose other conspirators or other criminal plans. We have used this approach to great effect in organized crime cases and espionage investigations, and members of our Safe Streets Task Forces use it in their fight against street gangs.

This is the approach that is needed to prevent terrorism. As of September 11, 2001, however, we were handicapped in our ability to implement this approach in the counterterrorism arena for two primary reasons.

- **First, judicial rules and DOJ internal procedures prohibited our counterterrorism agents working intelligence cases from coordinating and sharing information with criminal agents who often were working investigations against the same targets.**
- **Second, we had not developed the institutional structure and processes necessary for a fully functioning intelligence operation.**

We started to address each of these problems immediately after the September 11, 2001, attacks.

Integrating Criminal and Intelligence Operations

By definition, investigations of international terrorism are both "intelligence" and "criminal" investigations. They are intelligence investigations because their objective, pursuant to Executive Order 12333, is "the detection and countering of international terrorist activities," and because they employ the authorities and investigative tools – such as Foreign Intelligence Surveillance Act warrants – that are designed for the intelligence mission of protecting the U.S. against attack or other harm by foreign entities. They are criminal investigations since international terrorism against the U.S. constitutes a violation of the federal criminal code.

Over the past two decades, a regime of court rules and internal DOJ procedures developed surrounding the use of FISA warrants that barred FBI agents and other Intelligence Community personnel working intelligence cases that employed the FISA tool from coordinating and swapping leads with agents working criminal cases. As a result of this legal "wall," "intelligence" agents

and “criminal” agents working on a terrorist target had to proceed without knowing what the other may have been doing about that same target. In short, we were fighting international terrorism with one arm tied behind our back.

The USA PATRIOT Act, enacted on October 26, 2001, eliminated this “wall” and authorized coordination among agents working criminal matters and those working intelligence investigations. On March 6, 2002, the Attorney General issued new Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI *(Intelligence Sharing Procedures)* to capitalize on this legislative change. The new procedures specifically authorized agents working intelligence cases to disseminate to criminal prosecutors and investigators all relevant foreign intelligence information, including information obtained from FISA, in accordance with applicable minimization standards and other specific restrictions *(originator controls)*. Correspondingly, they authorized prosecutors and criminal agents to advise FBI agents working intelligence cases on all aspects of foreign intelligence investigations, including the use of FISA.

On November 18, 2002, the Foreign Intelligence Surveillance Court of Review issued an opinion approving the Intelligence Sharing Procedures, thereby authorizing us to share information, including FISA-derived information, between our criminal and intelligence investigations. With this opinion, we finally were free to conduct our terrorism investigations with the full use and coordination of our criminal and intelligence tools and personnel.

To formalize this merger of intelligence and criminal operations, we have abandoned the separate case classifications for "criminal" international terrorism investigations (*with the classification number 265)* and "intelligence" international terrorism investigations *(classification number 199)*, and we have consolidated them into a single classification for "international terrorism" *(new classification number 315)*. This reclassification officially designates an international terrorism investigation as one that can employ intelligence tools as well as criminal processes and procedures. In July 2003, we codified this approach in our Model Counterterrorism Investigative Strategy, which was issued to all field offices and has been the subject of extensive field training.

With the dismantling of the legal "wall" and the integration of our criminal and intelligence personnel and operations, we now have the latitude to coordinate our intelligence and criminal investigations and to use the full range of investigative tools against a suspected terrorist. On the intelligence side, we can conduct surveillance on the suspected terrorist to learn about his movements and identify possible confederates; we can obtain FISA authority to monitor his conversations; and/or we can approach and attempt to cultivate him as a source or an operational asset. On the criminal side, we have the option of incapacitating him through arrest, detention, and prosecution. We decide among these options by continuously balancing the opportunity to develop intelligence against the need to apprehend the suspect and prevent him from carrying out his terrorist plans. This integrated approach has guided our operations during the past 31 months, and it has successfully foiled terrorist-related operations and cells from Seattle, Washington, to Detroit, Michigan, to Lackawanna, New York.

Integrating Intelligence Processes in our Operations

Although we are now able to coordinate our intelligence collection and criminal law enforcement operations, we can only realize our full potential as a terrorism prevention agency by developing the intelligence structure, capabilities, and processes to direct those operations. Without an effective intelligence capacity, we cannot expect to defeat a sophisticated and opportunistic adversary like al-Qa’ida.

For a variety of historical reasons, the Bureau had not developed this intelligence capacity prior to September 11, 2001. While the FBI has always been the world's best collector of information, we never established the infrastructure to exploit that information fully for its intelligence value. Individual FBI agents have always analyzed the evidence in their particular cases, and then used that analysis to guide their investigations. But the FBI, as an institution, had not elevated that analytical process above the individual case or investigation to an overall effort to analyze intelligence and strategically direct intelligence collection against threats across all of our programs.

The attacks of September 11, 2001, highlighted the need to develop an intelligence process for the Counterterrorism Program and the rest of the Bureau. Since then, we have undertaken to build the capacity to fuse, analyze, and disseminate our terrorism-related intelligence, and to direct investigation activities based on our analysis of gaps in our collection against national intelligence requirements. That effort has proceeded in four stages.

Stage 1 Initial Deployment of Analysts

Our first step was to increase the number of analysts working on counterterrorism. Immediately after the September 11, 2001, attacks, we temporarily reassigned analysts from the Criminal Investigative Division and Counterintelligence Division to various units in the Counterterrorism Division. In July 2002, 25 analysts were detailed from the CIA to assist our counterterrorism efforts. Many of these analysts provided tactical intelligence analysis; others provided strategic "big picture" analysis. All of them worked exceptionally hard and helped us analyze the masses of data generated in the aftermath of the September 11, 2001, attacks. These deployments were a temporary measure, but the progress made, the confidence gained, and the lessons learned during this period started us down the road toward a functioning intelligence analysis operation. We also established the College of Analytical Studies to help train and develop our own cadre of analysts.

Stage 2 Office of Intelligence

On December 3, 2001, we established the Office of Intelligence *(OI)* within the Counterterrorism Division. The OI was responsible for establishing and executing standards for recruiting, hiring, training, and developing the intelligence analytic workforce, and ensuring that analysts are assigned to operational and field divisions based on intelligence priorities. Recognizing that intelligence and analysis are integral to all of the Bureau's programs, in February 2003, we moved the OI out of the Counterterrorism Division and created a stand-alone OI, headed by an Executive Assistant Director, to provide centralized support and guidance for the Bureau's intelligence functions.

Stage 3 Intelligence Program

The next step in our intelligence integration was to elevate intelligence functions to program-level status, instituting centralized management and implementing a detailed blueprint for the Intelligence Program.

We articulated a clear mission for the Intelligence Program – to position the FBI to meet current and emerging national security and criminal threats by: **1)** aiming investigative work proactively against threats; **2)** building and sustaining enterprise-wide intelligence policies and capabilities; and **3)** providing useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities. We then set out to embed intelligence processes into the day-to-day work of the FBI, from the initiation of a preliminary investigation to the development of FBI-wide strategies.

The Intelligence Program has the following elements:

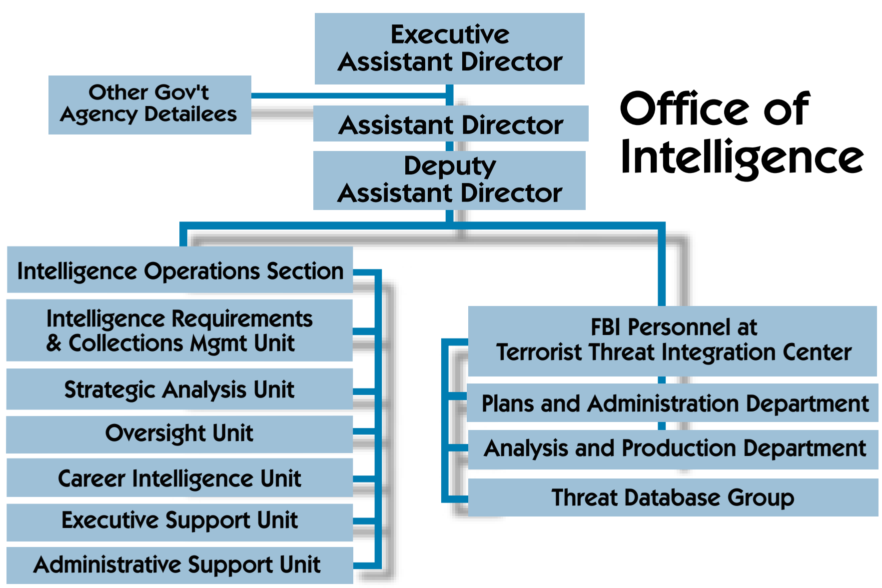
EAD Intelligence

In May 2003, our first Executive Assistant Director for Intelligence *(EAD-I)*, an intelligence expert with 25 years of experience in the Intelligence Community, joined the three other Executive Assistant Directors in the top tier of FBI management. The EAD-I is responsible for managing the national Intelligence Program, and for institutionalizing intelligence processes in all areas of FBI operations.

Primary responsibilities of the EAD-I are to:

- Establish, administer, and evaluate policies, guidelines, and standards governing all processes and products of the FBI Intelligence Program.
- Oversee the FBI's national collection requirements process; prioritize intelligence requirements; and evaluate field office performance against these priorities.
- Serve as the FBI's primary interface for the sharing of information with members of the intelligence, law enforcement, and international communities.

The EAD-I and the Assistant Director for the Office of Intelligence run the OI. The OI has two sections divided into units: the Intelligence Operations Section based at Headquarters, and the FBI contingent at the Terrorist Threat Integration Center *(TTIC)*, currently operating out of CIA Headquarters in Langley, Virginia. TTIC is discussed in more detail in the section on Coordination *(page 43)*.



Concepts of Operations

Between June and October 2003, we developed Concepts of Operations *(CONOPs)* for the various functions of the Intelligence Program. As these functions already were integral parts of established divisions, the OI brought together representatives from all parts of the FBI to assist in developing documents that satisfy needs throughout the Bureau.

The purpose of each CONOP is to build a shared vision of how the FBI will execute each intelligence function. The CONOPs identify guiding principles and policies, describe standards and procedures, allocate intelligence responsibilities, and create a shared intelligence vocabulary.

The CONOPs include:

- **Intelligence Requirement and Collection Management Process CONOP** *(August 2003)* – defines the process for promulgating intelligence needs and the collection taskings to meet those needs. Intelligence needs are articulated by many consumers, including the intelligence, homeland security, and law enforcement communities.
- **Intelligence Assessment Process CONOP** *(August 2003*) – defines a methodology for intelligence assessments that can be applied to any analytical product and is designed to ensure that FBI analytical products draw from all available sources, add value, and meet the needs of specific consumers.
- **Field Office Intelligence Operations CONOP** *(August 2003*) – defines a practical strategy for the implementation of intelligence processes in field divisions.
- **Human Talent for Intelligence Production CONOP** *(September 2003)* – lays out a strategy to continually develop, motivate, and retain the analytic work force. It describes our specific plans for the recruiting, hiring, career development, and training of analysts.
- **FBI Intelligence Production and Use CONOP** *(October 2003)* – defines authorities and responsibilities, and outlines a common approach, for producing intelligence within the FBI. It prescribes a common set of products and services that should be provided by FBI intelligence components, such as uniform Bureau-wide templates for Intelligence Assessments and Intelligence Bulletins. It also defines intelligence production policy.
- **FBI Information Sharing CONOP** *(March 2004)* – presents guiding principles and operational approaches for sharing information internally and externally.
- **Budget Formulation for Intelligence CONOP** (*February 2004)* – defines the budget formulation process for the FBI's Intelligence Program. The new process extends beyond the resources needed by the OI to do its job and includes those resources required by operating divisions to complete intelligence functions. It replaces the old process whereby intelligence-related resources were "stove-piped" within each operational division, and replaces it with an enterprise-wide approach to resource allocation based on an integrated threat forecast.
- **Intelligence Program CONOP** *(February 2004)* – provides a general overview of the Intelligence Program and spells out goals, objectives, and metrics for measuring success.
- **Customer Relations CONOP** *(nearing finalization)* – defines the FBI approach to working with consumers of FBI intelligence. Core principles include writing our products at the classification level of most use to the consumer.

Beginning in October 2003, managers from the OI and the operational divisions have met on a weekly and monthly basis to facilitate implementation of these CONOPs. Managers provide feedback on implementation problems and challenges, identify implementation tasks requiring cross-organization support, and ensure the consistency of policy guidance in all divisions.

Field Office Intelligence Operations

In order to ensure that FBI-wide collection plans and directives *(requirements, collection tasking, analysis, and dissemination)* are incorporated into field offices, on September 12, 2003, we directed all field offices to establish a Field Intelligence Group *(FIG)*. We followed up that directive with the issuance of formal guidelines for implementation and operation of FIGs on October 18, 2003. All field offices have established and are now operating FIGs.

The FIG is the centralized intelligence component in each field office, responsible for the management, execution, and coordination of intelligence functions. FIGs vary in size and structure according to the size of the division and other factors. An Assistant Special Agent in Charge *(ASAC)* in each field office is assigned responsibility for intelligence-related functions and has oversight of the FIG. The three field offices headed by an Assistant Director in Charge *(the New York, Los Angeles, and Washington Field Offices)* must have both an SAC and an ASAC so designated.

FIG personnel analyze and disseminate the intelligence collected in their field office. They conduct intelligence assessments and generate intelligence products in accordance with the FBI's Intelligence Assessment Process CONOP and other intelligence production guidelines. They also support the 24-hour intelligence cycle of the FBI by employing all appropriate resources to drive the collection and dissemination of threat information, investigative developments *(urgent reports)*, and other significant intelligence to meet the information needs of all consumers.

Requirements Process

FBI agents have always been excellent collectors of information, but this ability to gather information was never fully integrated into an FBI-wide process for identifying and collecting needed intelligence. The Counterintelligence Division has long operated according to a centralized requirements-driven process for the collection and analysis of intelligence, and that capacity has been critical to its successes over the years against Soviet spying, economic espionage, and other efforts to steal our national secrets and penetrate our institutions. However, because counterintelligence traditionally was conducted without significant overlap with other Bureau programs, that intelligence capacity largely remained limited to the Counterintelligence Program.

Since September 11, 2001, we have expanded this requirements process by establishing a formal FBI-wide process for promulgating intelligence requirements and issuing appropriate collection taskings to operational divisions both at Headquarters and in the field. These requirements derive from the National Intelligence Priorities Framework as approved by the National Security and Homeland Security Councils. The new requirements process ensures that a continuing cycle for determining where we have intelligence gaps and targeting our information collection activities to fill those gaps. This cycle takes place at both the field and Headquarters levels and has four steps:

Step 1 – Finding out what we know and don't know

First, we survey all available intelligence across the organization, including intelligence from outside partners, to determine where we have intelligence gaps. These gaps, also known as intelligence requirements, are unanswered questions that we need to answer if we are to have a complete picture of threats in priority areas. The OI consolidates these gaps and communicates them to supervisors and analysts throughout the Bureau. Analysts in Headquarters operational divisions and in each FIG, tap into all available sources to try to resolve the gaps.

Step 2 – Directing collection to fill the gaps

After the analysts have completed this process, the next step is to collect the information we need to resolve the intelligence gaps that remain. At Headquarters, the OI issues reports listing the remaining gaps. Based on these lists, investigators on squads, in resident agencies, and on task forces are then tasked to collect the needed information using all available investigative tools, including cultivation of new sources. In instances where a national information gathering effort is required, collection may be coordinated through the NJTTF, bringing the significant resources of our federal, state, and municipal partners to bear on the problem.

Step 3 – Answering the questions

Once we have gathered sufficient information to resolve a particular gap, agents and analysts consolidate and analyze the information collected and generate intelligence products for the widest possible audience. Intelligence Information Reports *(IIRs)* are issued to share raw intelligence. Intelligence Assessments are issued to share value-added assessments of criminal or national security threats.

Step 4 – Ensuring the answers get to the right people

The final step is to share those intelligence products as widely as possible. Dissemination is coordinated by Headquarters intelligence entities and by FIGs in the field.

Baselining of Sources

On December 15, 2003, we directed all field offices to enter information into a database on every collection source they have, the source's history and motivation for working with us, and what information that source is providing. This effort is helping us to know what sources we have, what we should be reporting in intelligence products from those sources, and where we have key gaps in our collection capability that must be filled through targeted collection strategies.

Analytical Assets

Since September 11, 2001, we have taken a number of important steps to build an analytic workforce capable of addressing the new threat environment.

Hiring—We have hired 460 analysts, and we are working to hire hundreds more in 2004. We also implemented a comprehensive recruitment strategy for analysts that includes a targeted marketing plan, development of a team of 20 analysts trained to serve as analyst recruiters, and a new tuition reimbursement plan.

Training—We created the College of Analytical Studies to provide analysts with a formal training program. The curriculum was developed with recommendations and participation from the CIA's Sherman Kent School, the Joint Military Intelligence College and private educational institutions. In FY 2003, the College of Analytical Studies trained 932 FBI and 14 DOJ personnel. The training consisted of basic and advanced courses at Quantico, as well as CIA courses for FBI personnel in the field.

The Analyst Position—There are three separate roles for the analyst position:

- **Operations Specialists** provide critical front line intelligence support to investigations in the field and at FBI Headquarters, as well as case management assistance.
- **Reports Officers** identify and extract essential information and analysis from FBI Investigations and intelligence products, and they synthesize the information into disseminable reports that are shared with appropriate FBI entities, law enforcement agencies, and the Intelligence Community. This new position in the FBI is vital to our efforts to maximize the amount of information shared with our partners.
- **All-Source Analysts** examine data to find patterns and associations, use that knowledge to predict threats, and generate products to help investigators and decision-makers better understand and respond to present and future threats.

The Analyst Career Track—We instituted an analyst career track that offers analysts three choices. After analysts reach a certain level of seniority *(the GS-11 level)*, they are asked if they are interested in: **1)** building expertise in a specific program area *(such as al-Qa'ida)*; **2)** gaining broader experience that will prepare them to work in a number of program areas; or **3)** working toward becoming a supervisor or manager in the Intelligence Program. Training and temporary assignments appropriate to a particular track are first offered to analysts in that track.

Supervision—The OI establishes and implements standards for recruiting, hiring, training, and developing our analysts, and ensures that they are assigned to operational and field divisions based on intelligence priorities. Operational and field divisions are responsible for day-to-day supervision of analysts and for adhering to the standards for analyst development established by the OI.

On February 1, 2004, we established a reporting structure that institutionalizes this shared responsibility, ensuring that the OI has sufficient supervisory authority over analysts, and particularly over the analyst supervisors. Under this structure, analysts report to and receive their annual evaluations from their operational supervisors, and the OI reviews and signs off on those evaluations. Section Chiefs who oversee analysts at Headquarters report to and receive their annual evaluations from officials in the OI, and their evaluations are reviewed by supervisors in the Headquarters investigative division into which they are integrated.

This reporting structure ensures that analysts remain embedded in their investigative units and responsive to operational needs while also being subject to supervision and deployment in accordance with the Bureau's overall intelligence requirements process. It also gives the OI the necessary authority to implement its intelligence processes through the analyst supervisors.

Intelligence Production Board

We established an FBI Intelligence Production Board to ensure that timely decisions are made regarding the production and dissemination of all analytical products. The Board is made up of representatives from each Headquarters operational division, the OI, the FBI Laboratory, the Office of Law Enforcement Coordination, and DHS representatives, and is chaired by the EAD-I. The Board holds daily meetings to review significant threats, developments, and issues emerging in each investigative priority area, and to identify topics for intelligence products.

Stage 4 Intelligence Workforce

Now that the Intelligence Program is established and developing, we are turning to the next stage of transforming the Bureau into an intelligence agency – reformulating our personnel and administrative procedures to instill within our workforce an expertise in the processes and objectives of intelligence work.

We recently issued five directives that will fundamentally reorient the development of our entire workforce toward the intelligence mission. From recruitment to training to career advancement to the evaluation of personnel and programs, these initiatives will transform our administrative and personnel systems to ensure that intelligence objectives are paramount in our plans and performance. Some components of these initiatives have already been implemented; some are in advanced stages of development; and others are in the early planning stages.

The following summarizes these initiatives:

Recruitment

We are targeting our recruitment efforts to attract agent and analyst candidates with Intelligence Community or other intelligence experience, or with backgrounds in international studies and international finance. We sought input from other Intelligence Community agencies to determine "best practices" for successfully recruiting individuals with intelligence-related skills, and we incorporated these best practices into new recruiting plans for Special Agents and analysts. We are recruiting at colleges and universities with outstanding academic programs in intelligence-related disciplines. In addition, since one of the richest fields for intelligence backgrounds is military intelligence, we are soliciting the services of an experienced contractor who specializes in placing military officers and enlisted candidates who possess intelligence expertise.

Special Agent Career Tracks

Traditionally, the Bureau has recruited, trained, rewarded, and promoted its agents primarily for law enforcement work. This approach was adequate so long as the Bureau's mission was perceived largely as law enforcement. It is no longer adequate now that intelligence work has assumed such a central role in our efforts to prevent terrorism.

On March 22, 2004, we established a new career path for Special Agents designed with three objectives. First, the career path will give all agents experience with intelligence and analysis. Second, the career path will give agents an opportunity to develop specialized skills, experience, and aptitudes in one of the four program areas: **1)** Intelligence; **2)** Counterterrorism/Counterintelligence; **3)** Cyber; or **4)** Criminal. Third, it makes intelligence expertise and experience a prerequisite for elevation to senior supervisory ranks.

This plan will produce a cadre of agents who are proficient in the processes of intelligence collection, but who also have the law enforcement powers to take advantage of our integrated operational approach.

This career track will take Special Agents through the following stages:

First Assignment

We reinstituted the FBI's traditional Rotational Transfer Policy to expose new agents to a wide range of field experience, and then help them progress to more specialized skills to handle complex investigative and intelligence responsibilities. Most new agents will be assigned for the first three years to one of the smallest 41 FBI field offices. Assignment to smaller offices and to positions in each of the four program areas will

give them exposure to a wide range of training and experiences and help them develop core investigative and intelligence competencies under the guidance of experienced agents. This initial tour of duty will ensure that all agents have strong intelligence backgrounds and are well versed in all of the FBI's operational programs.

As part of their broad training during the first three years, new agents will be required to complete an assignment in a FIG or a Headquarters intelligence entity. This will be an important step in an agent's development. It will sensitize them to the importance of analysis and analysts, and it will give them an understanding of the tools and processes of intelligence analysis and production.

Second Assignment

After approximately three years, agents will be transferred to one of the 15 largest FBI field offices with primary assignment to an area of specialization. They will receive continuing advanced training tailored to their areas of specialization and become familiar with handling the substantial threats we encounter in large metropolitan areas. An increasing number of these agents will specialize in intelligence or counterintelligence/counterterrorism.

Intelligence Officer Certification

We will also develop and implement a process for Special Agents to receive a formal Intelligence Officer Certification. Drawing on the model in the Intelligence Community, this process will grant certification to Special Agents who complete a set of minimum requirements related to advanced training, assignments and experience, and/or formal education. The experience requirement can be met through a combination of intelligence training and a detail assignment with another member of the Intelligence Community, assignments to the OI or FIGs, or prior intelligence experience or education. This certification can be earned by any agent who meets the requirements, regardless of their primary areas of specialization. For example, an agent on the criminal career path can complete the requirements for Intelligence Officer Certification and use the knowledge and expertise he or she gains to integrate intelligence into criminal investigations.

Promotion to Upper-Level Management

Once the Intelligence Officer Certification process is established, this certification will become a prerequisite for promotion to the rank of Assistant Special Agent in Charge or to a Section Chief position in any investigative division at FBI Headquarters or the OI – entry positions to the FBI's upper-management. This requirement constitutes a revolutionary change in our promotion policies, and will ensure that all future entrants to the FBI's upper management are fully trained intelligence officers.

Training

Training programs that focus on the skills and knowledge necessary for counterterrorism and counterintelligence investigations and intelligence functions are a critical element of the FBI's transformation. With numerous initiatives either already implemented or in the works, we are making intelligence-based training a part of FBI agents' and support employees' careers from their first day on the job to their last.

Training initiatives to date include the following:

New Agents Training

We extended new agents training from 16 weeks to more than 17 weeks to allow for the expansion of classroom instruction in counterterrorism and counterintelligence from 55 hours to 110 hours. We reworked the traditionally law enforcement-focused program to emphasize how intelligence and criminal investigative techniques are used in tandem as part of the FBI's re-ordered strategic mission. We are emphasizing development of an intelligence base through the operation of human sources and liaison with other agencies.

We are inserting the following areas of instruction into the new agents training curriculum:

- **FBI intelligence mandates and authorities**
- **Overview of the intelligence cycle**
- **Introduction to the U.S. Intelligence Community**
- **Intelligence reporting and dissemination**
- **FBI intelligence requirements and the collection management process**
- **Role of intelligence analysts**
- **Validating human sources**

In addition, advanced intelligence and national security training integrated with the College of Analytical Studies will be required for agents with Intelligence and Counterterrorism/Counterintelligence skill designations.

In-Service Training

We have developed a number of training programs for on-board employees, including the following:

FISA/USA PATRIOT Act Training

The FBI partnered with the DOJ and the CIA to develop and present a multimedia curriculum that has trained approximately 3,800 FBI agents and analysts, members of our Joint Terrorism Task Forces, and Assistant United States Attorneys on new legal and operational requirements, processes, and tools related to counterterrorism and other national security investigations.

Language Training

In fiscal year 2003, the FBI’s Foreign Language Training Program provided training and/or self-study materials to almost 1,800 employees in 32 languages. We also partnered with the Foreign Service Institute to develop and sponsor language training and foreign-duty instruction that has provided 6,200 hours of training to 172 FBI employees over the past two years.

Human Source Recruitment

All FBI Special Agents recently received a mandatory three-hour block of "Back to Basics" refresher training on human source recruitment, development, and management.

University Education Program

The FBI established a tuition reimbursement program to enable qualified employees in the Counterterrorism, Counterintelligence, Cyber, and Security Programs to get advanced degrees.

Looking forward, we are in the process of implementing the following:

- We are incorporating into new agent training more practical exercises in which trainees task intelligence analysts and use intelligence products in the course of their mock investigations.
- We are developing specialized and advanced training for Special Agents, tied to Intelligence, Counterterrorism/Counterintelligence, Cyber, and Criminal career paths. This training is being developed and presented on a phased-in basis, with the intelligence career path training as the first priority.
- We are designing a training development plan for advanced and specialized intelligence training necessary for Intelligence Officer Certification.
- We are working to integrate intelligence-related topics throughout all in-service agent training.
- We are developing computer-based training on the integration of intelligence and policing. This effort is a collaboration among federal, state, and municipal law enforcement representatives, who will put forth a "model" to be used by all law enforcement as the benchmark for intelligence and policing. The planned CD/DVD will be a key distance learning resource for agents and other FBI employees, as well as for the FBI's partners in state and municipal law enforcement.
- We are developing new courses supporting counterterrorism operations that will be delivered through a combination of classroom instruction and web-based training on our intranet. Classes currently under development include:

  Developing Sources
  Understanding Islam and the Arab Culture
  Reports Officers and Counterterrorism
  Advanced Surveillance and Counter-surveillance Techniques
  National Security Investigation Attorney General Guidelines
  National Security Investigation Tools and Techniques
  Terrorism Screening Center Tools

Program Evaluations

If the FBI's continuing transformation is to succeed, it is vital that we provide not only the necessary tools, but also appropriate guidance and motivation. We can no longer evaluate our programs solely on the basis of case-focused measures such as the number of indictments and convictions. Accordingly, we have developed new standardized metrics to evaluate the performance of the Counterterrorism, Counterintelligence, Cyber, and Criminal Investigative Programs. The new metrics will encourage the proactive activities, information gathering, and coordination with partners needed to build a strong intelligence base. For example, the Counterterrorism Program now will be evaluated, in part, on the quality of its threat assessments, the development of human and other sources of information that contribute to the intelligence base, and its information sharing and liaison activities. Beginning in October 2004, program coordinators in each field office will be required to conduct semi-annual program reviews using the new metrics.

The new semi-annual program reviews will be used in several ways. Field office and program managers will use them to assess their performance and to identify the strengths and weaknesses of their programs so that they can institute improvements. Program managers at Headquarters will examine the results of these reviews, identify national or individual field office performance issues, and recommend corrective action as needed. The Inspection Division will analyze the semi-annual reviews in preparation for regularly scheduled inspections. The Inspection Division also will use the reviews to determine if there are any performance anomalies that may require an unscheduled inspection.

Similarly, we modified the inspection criteria for field offices to include performance metrics for their intelligence programs. The intelligence components in each field office will be monitored to ensure that intelligence information is managed and disseminated quickly and in a format for use by other members of the Intelligence Community.

Special Agent Evaluations

Special Agents currently are evaluated according to specified performance criteria related to eight "critical elements." These elements provide guidance and define the activities we expect an agent to undertake and master.

On March 22, 2004, the Director approved a proposal to revise the evaluation criteria for all Special Agents to emphasize intelligence objectives. The proposal would create a new Critical Element 7, "Intelligence Collection and Reporting," to require that each agent demonstrate and effectively apply knowledge, authorities and mandates governing intelligence functions. We also propose revising Critical Element 8, "Developing an Intelligence Base," to ensure that agents effectively cultivate and exploit intelligence sources.

Proposed Critical Element 7: Intelligence Collection and Reporting

- Demonstrates and independently applies effective knowledge of authorities and mandates governing the intelligence functions of the FBI.
- Demonstrates and independently applies broad knowledge and awareness of the needs of FBI intelligence customers and partners in other federal law enforcement agencies; the state, local, and tribal law enforcement communities; the U.S. Intelligence Community; and/or friendly foreign services, and serves these needs effectively.
- Independently collects intelligence of value in accordance with prevailing sets of intelligence requirements, using all appropriate investigative and intelligence collection techniques.
- Independently ensures that collected raw intelligence is reported in accordance with established guidelines to relevant customers, both internally and externally, through all appropriate means, to include effective interaction with the Field Intelligence Group.
- Independently ensures that intelligence analysts receive all relevant collected intelligence to effectively support the FBI's intelligence analysis and production responsibilities.

Proposed Critical Element 8: Developing an Intelligence Base

- Independently identifies and effectively operates human sources in accordance with prevailing sets of intelligence requirements, and makes sound judgments regarding the value of their contributions.

- Independently establishes and maintains effective liaison relationships with individuals or organizations to facilitate the intelligence process, and in accordance with prevailing sets of intelligence requirements.
- Independently obtains, analyzes, and reviews information *(record checks)* regarding the suitability of individuals for use in intelligence collection and investigations.
- Independently submits accurate and timely documentation, reports, and communications regarding human source operation and intelligence collection through liaison.

These new critical elements will go into effect only once they are reviewed and validated according to the procedures governing our personnel evaluation process.

Evaluation of Special Agents in Charge

Historically, the Assistant Director of the Criminal Investigative Division has served as the rating official for SACs and Assistant Directors in Charge *(ADICs)* of the Los Angeles, New York and Washington Field Offices. In February 2004, we issued a new policy whereby the responsibility for rating ADICs and SACs will rotate annually among the ADs of the operational divisions, with input provided from the AD of the Office of Intelligence. The rating official for ADICs and SACs will be the AD for Counterterrorism the first year; the AD for Cyber the second year; the AD for Counterintelligence the third year; and the AD for Criminal Investigations the fourth year. This change, scheduled to go into effect on October 1, 2004, will afford more broad-based performance oversight and eliminate any undue emphasis on any one investigative program.

COORDINATION

A major element of the Bureau's transformation is our increasing integration and coordination with our partners in the U.S. and international law enforcement and intelligence communities. More than any other type of enforcement mission, counterterrorism requires the participation of every level of local, state, national, and international government. A good example is the case of the Lackawanna terrorist cell outside Buffalo, New York. From the police officers who helped to identify and conduct surveillance on the cell members; to the CIA officers who provided information from their sources overseas; to the diplomatic personnel who coordinated our efforts with foreign governments; to the FBI agents and federal prosecutors who conducted the investigation leading to the arrests and indictment, everyone played a significant role.

We recognize that a prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that allow information sharing on a regular and timely basis, we and our partners cannot expect to align our operational efforts to best accomplish our shared mission. Accordingly, we have taken steps to establish unified FBI-wide policies for sharing information and intelligence.

The Role of the Executive Assistant Director for Intelligence

To ensure a coordinated, enterprise-wide approach, the Director recently designated the EAD-I to serve as the principal FBI official for information and intelligence sharing policy. In this capacity, the EAD-I serves as advisor to the Director and provides policy direction on information and intelligence sharing within the FBI and outside the FBI with the law enforcement and intelligence communities, as well as foreign governments.

Information Sharing Policy Group

On February 20, 2004, we formed an information sharing policy group, comprised of Executive Assistant Directors, Assistant Directors and other senior executive managers. Under the Direction of the EAD-I, this group is establishing FBI information and intelligence sharing policies.

Department of Justice Intelligence Coordinating Council

On February 11, 2004, the Attorney General announced the creation of the DOJ Intelligence Coordinating Council. The Council is comprised of the heads of DOJ agencies with intelligence responsibilities, and is currently chaired by the FBI's EAD-I. The Council will work to improve information sharing within DOJ and to ensure that DOJ meets the intelligence needs of outside customers and acts in accordance with intelligence priorities. It will also identify common challenges *(such as electronic connectivity, collaborative analytic tools, and intelligence skills training)* and establish policies and programs to address them.

Beyond these information sharing initiatives, we are increasing our operational coordination with our state, federal, and international partners on a number of fronts.

State and Municipal Law Enforcement

We have taken many steps to continue to improve our relationships with the approximately 750,000 men and women of state and municipal police departments around the country. Many

have started to take note of these efforts. For example, New York City Police Commissioner Raymond W. Kelly testified at the Commission's March 31, 2003, public hearing as follows:

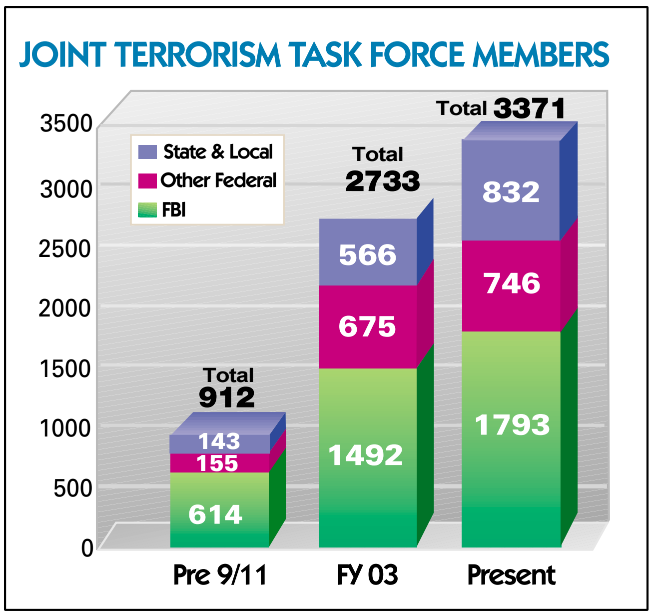
> ***"I have been in law enforcement a long time, both on the federal and the local level. And clearly there were some issues in the past with the flow of information. I can tell you that has changed significantly in the aftermath of September 11th ….There is a palpable difference in [the FBI's and CIA's] approach to doing business. They want to get that information out. They are getting it out."***

This critical improvement is the direct result of new and expanded collaborative efforts, innovative approaches to information sharing, new policies and technologies, and above all a commitment to support our partners in law enforcement. We have worked closely with our partners as we developed and implemented these changes, seeking input and feedback each step of the way.

While there is still progress to be made, these efforts have produced a higher level of coordination in our working relationship with state and municipal law enforcement. This coordination is reflected in the following areas:

Task Forces

The FBI has long relied on strong operational relationships with state and municipal law enforcement. We work in partnership on a wide range of task forces, to include Safe Streets Task Forces that fight violent street gangs, Crimes Against Children Task Forces, Financial Institution Fraud and Identity Theft Task Forces, Health Care Fraud Task Forces, Organized Crime Drug Enforcement Task Forces *(OCDETF),* Major Theft Task Forces, Safe Trails Task Forces that fight violent crime in Indian Country, and case specific task forces related to serial murders, hate crimes, and other types of criminal activity. FBI personnel on these task forces work side-by-side with their local counterparts to solve crimes and improve the level of safety and security in their communities. This day-to-day interaction has forged relationships that we rely on in our joint efforts to combat terrorism. Those established relationships have been the foundation of our Joint Terrorism Task Forces, which are the keystone of our counterterrorism efforts.



JTTFs team up police officers, FBI agents, and officials from over 20 federal law enforcement agencies to investigate terrorism cases. Since September 11, 2001, we have expanded the JTTFs to every field office in the country and to 28 resident agencies – increasing the total number of JTTFs from 34 to 84. We have also established Executive Boards in each field office made up of FBI executive managers and the heads of law enforcement agencies represented on the JTTFs. These JTTFs have been a resounding success, and they play a central role in virtually every terrorism investigation, prevention, or interdiction within the U.S.

Office of Law Enforcement Coordination

We established the Office of Law Enforcement Coordination *(OLEC)* in the spring of 2002 to strengthen relationships between the FBI, state and municipal law enforcement, and other federal law enforcement agencies. The OLEC works closely with law enforcement groups such as the International Association of Chiefs of Police and the Fraternal Order of Police, provides a voice for these groups within the Bureau, and gives them a place at the decision making table when law enforcement and prevention strategies are being developed.

We selected a former Chief of Police to be Assistant Director in charge of OLEC and located him in an office near the Director. The Assistant Director has decades of experience in law enforcement and has earned a reputation for building bridges within the law enforcement community. He has developed a number of initiatives to enhance coordination through his office, including:

Director's Law Enforcement Advisory Group (DLEAG)

The DLEAG, comprised of the heads of the national law enforcement organizations, meets regularly with senior FBI executives to provide input on various issues of common concern. Issues discussed at recent meetings include: **1)** the issuance of Homeland Security "alerts" and the impact on state and local agencies when threat advisory levels are raised; **2)** the FBI's investigative priorities; **3)** state and local law enforcement counterterrorism needs; **4)** ways to enhance communication within law enforcement; and **5)** recommended improvements of the training at the National Academy.

FBI Police Executive Fellowship Program (EFP)

In 2002, OLEC started the EFP to give high-ranking state and local law enforcement managers an opportunity to spend six months working in an FBI Headquarters program such as the NJTTF or the Office of Intelligence. The four officers who have participated to date have brought vital law enforcement perspectives to Headquarters and have made important contributions to our information and intelligence sharing efforts.

Community Oriented Policing Training

OLEC has worked closely with the Training and Development Division to revise the new agents training curriculum to incorporate Community Oriented Policing concepts. Agent trainees learn that a high level of involvement with the community is expected and required if they are to succeed in their jobs.

Terrorism Quick Reference Card (TQRC)

One small, but practical, initiative is our TQRC reference guide. The guide is designed to fit into the overhead visor of police vehicles and lists suspicious factors that may indicate ongoing terrorist activity. To date, 430,000 TQRCs have been distributed to state and municipal law enforcement officers.

Terrorist Screening Center

On September 16, 2003, the President directed the Attorney General, Secretary of Homeland Security, Secretary of State, and Director of Central Intelligence to develop the Terrorist Screening Center *(TSC)* to consolidate information from terrorist watch lists and provide 24-hour, seven-days-a-week operational support for law enforcement, consular officers and other officials. The FBI was directed to lead this effort and to begin operations by December 1, 2003. Thanks to significant contributions by all participating agencies, operations began – and continue to develop – on schedule.

The TSC performs the following functions: **1)** it receives identity information of potential terrorists (*name and identifying information*) from different government agencies; **2)** it merges that identity information into the Terrorism Screening Database, which is used to assist the police officer, border official, or consular official in making a positive identity match with a known or suspected terrorist; and **3)** if there is a potential match with a known or suspected terrorist, the TSC passes the information to the Bureau's CT Watch, which then coordinates the operational response through the local JTTF.

For example, when a police officer on patrol encounters an individual and runs his or her name through the National Crime Information Center *(NCIC)* system, the system now includes a check against TSC's list of persons with known or suspected links to terrorism. If that officer gets a "hit" or match against the database, the officer receives prepared instructions such as "arrest," "detain," or "question the individual." The officer is also instructed to call the TSC's 24/7 call center, which assists in the identity match of the person encountered, and connects the officer to CT Watch and the appropriate JTTF for further actions and investigation.

From December 1, 2003, through March 23, 2004, the TSC received 2,045 calls from state, federal, and local law enforcement personnel, based on potential matches with known or suspected terrorists. These calls resulted in 835 positive identifications, some of whom have been apprehended on various charges while others have been developed into informants or subjected to surveillance. The following two are examples:

- ***A local department contacted the TSC following a an NCIC "hit" after an arrest on a minor charge. TSC contacted the local JTTF, who interviewed the subject regarding his involvement with a domestic terrorist group. The subject agreed to cooperate with the FBI and is now an informant on domestic terrorism matters.***

- ***Local police arrested the subject of a an NCIC "hit" and found evidence in his vehicle that indicated surveillance of a possible terrorist target. They contacted TSC, who confirmed the person's identity and contacted the local JTTF, which then expanded its existing investigation.***

Law Enforcement Online

Law Enforcement Online *(LEO)* is a 24 hours a day, seven days a week, real-time, interactive computer communications and information service – an Internet for the law enforcement, criminal justice, and public safety communities. Over the past 31 months, we have expanded our use of LEO to facilitate information sharing with state and municipal law enforcement and first responders. For example, the NJTTF and all of the JTTFs have established Special Interest Groups on LEO, accessible to all law enforcement personnel, to facilitate the exchange of terrorism information nationally and locally. We also interfaced LEO with two other law enforcement networks: **1)** the National Law Enforcement Telecommunications System *(NLETS)*, an information sharing network that connects state, municipal, and federal law enforcement and justice agencies; and **2)** the Regional Information Sharing Systems Network *(RISS)*, that provides law enforcement users with database pointer systems, investigative leads bulletin boards, and encrypted e-mail.

Interconnectivity among the combined users of LEO, NLETS, and RISS gives us the means to share information with more law enforcement partners, more quickly, and with greater ease than ever before.

Alert Notification System

In June 2003, we launched a new Alert Notification System to notify police chiefs or local command centers of alerts, threats, or other critical information. Push technology pops messages up on computers – like instant messaging, but in a secure environment – and sends alert notifications to the chiefs' cell phones and pagers. The system can deliver the message selectively to specific groups *(as dictated by geography or function, such as border states or airport security)* or broadcast it to all possible recipients. Messages can include text, photos, and maps.

Intelligence Bulletins

Since September 11, 2001, the Counterterrorism Division has issued over 100 Intelligence Bulletins to state and municipal law enforcement agencies through the NLETS, e-mail, or facsimile. These weekly Intelligence Bulletins share information from all sources that may aid the recipients in preparing for and responding to security threats in their areas. The information in the bulletins is primarily intended for use by patrol officers and other law enforcement personnel who may encounter situations or information through their direct contact with the general public.

Information Sharing Pilot Projects

Ongoing pilot projects are helping us test new concepts for improving information sharing and coordination with our state and local partners around the country.

- **The Gateway Information Sharing System** integrates unclassified FBI criminal information with various forms of data – including police reports and narratives and calls for service records – from participating federal, state, and local agencies in the St. Louis region. This effort provides participating law enforcement entities with a single source for investigative lead material from a wide region, and the ability to search the text of various records for names, addresses, phone numbers, vehicles, and other data.
- **The Law Enforcement National Data Exchange *(N-DEx)*** is an information tool that serves as an index and pointer to help investigators make the most of data in existing repositories to examine relationships between criminal incidents. A prototype system has been designed and is scheduled for delivery in June 2004.
- **The Counterterrorism Reporting System on Suspicious Surveillance *(CROSS)*** is a new database being piloted in the National Capital Region. CROSS documents instances where individuals appear to be engaged in suspicious surveillance. The data is entered into the system via LEO and can then be analyzed and checked against other intelligence information by the local JTTF.

Security Clearances

In most cases, the FBI can provide information to our law enforcement partners in an unclassified form that can be widely distributed. However, there remain instances where law enforcement personnel require a Secret or Top Secret level clearance in order to perform their duties. Secret and Top Secret security clearances can only be granted after a thorough background check is conducted. These checks are labor intensive and require the skills of experienced investigators.

In December 2002 we established a new policy to grant prospective JTTF members and law enforcement executives an interim security clearance while the background check for permanent clearance is conducted. To expedite the background checks, in February 2003, we created a new unit within the Security Division to focus on security clearance processing for law enforcement executives and JTTF members. We also put new procedures in place and reassigned personnel from other FBI security programs. These priority requests for clearance are now completed, in most cases, within 180 days.

Between September 11, 2001, and February 19, 2004, the Security Division received and processed the following:

State and Local Law Enforcement Executives

2,707 security clearance requests received

2,351 successfully processed
(87 discontinued or administratively closed)

269 open cases currently pending

Joint Terrorism Task Force Members

1,589 requests for Top Secret clearance

1,414 successfully processed

175 open cases currently pending

New Counterterrorism Training Initiatives

Following September 11, 2001, we recognized the need to train not only our own employees, but also our state and municipal law enforcement partners, to meet the challenge of international terrorism. Several new or updated training efforts are helping us share counterterrorism expertise and knowledge about terrorist activities.

State and Local Anti-Terrorism Training (SLATT)—SLATT is a new training initiative mandated by the USA PATRIOT Act. In partnership with DOJ's Bureau of Justice Assistance and the Institute for Intergovernmental Research, we developed a national counterterrorism "Train the Trainer" program. From February 2003 to May 2003, Institute instructor teams provided 200 FBI instructors with a counterterrorism "Train the Trainer" course. These 200, in turn, trained 25,036 police officers from April 1, 2003, through December 31, 2003, with minimal cost. This highly successful initiative not only raised the level of counterterrorism expertise among our state and municipal partners; it also gave our field agents an opportunity to interact with local officers and improve their professional relationships.

National Academy—Since 1935, the FBI has offered the National Academy program to experienced law enforcement managers nominated by their agency heads because of their leadership qualities. Over the past 31 months, 2,220 state, municipal, and federal law enforcement personnel have received training – including counterterrorism instruction – through the National Academy.

Field Office Initiated Training— Counterterrorism training is being provided by individual field offices to state and local law enforcement personnel in their regions.

Weapons of Mass Destruction *(WMD)* Training— FBI personnel are providing training related to WMD at the DHS's Center for Domestic Preparedness.

Behavioral Analysis Unit

The FBI has long provided the law enforcement community with behavioral analysis support and advice in a variety of investigative matters, such as child abduction cases and serial murders. We are now lending similar expertise and assistance in terrorism-related matters. In July 2003, we established a new behavioral assessment unit in the Critical Incident Response Group at the National Center for Analysis of Violent Crime, to provide behavioral analysis support on matters involving terrorism and threatening communications, bombings, stalkings, arsons, and anticipated or active crisis situations. It also provides training and identifies behaviorally focused anti-terrorism research projects to enhance operational, investigative and preventive measures. In addition, we established a Communicated Threat Assessment Database *(CTAD)* which, when populated with historical and current case information, will serve as the repository for all communicated threats submitted to the new unit for analysis and as a resource to help evaluate new threats. Currently, the CTAD contains approximately 1,000 communicated threats received for analysis.

Regional Computer Forensic Laboratory Program

The Regional Computer Forensic Laboratory *(RCFL)* Program is another ongoing initiative designed to enhance our working relationships with state and municipal police departments around the country. This program establishes laboratory facilities that conduct forensic examinations of digital media to support investigations and prosecutions. RCFLs also conduct training. In FY 2003, the four operational RCFLs conducted 68 separate classes and trained 1,432 law enforcement officers. RCFLs are operated jointly by the FBI and other law enforcement agencies operating within a geographic area. The FBI opened new facilities in Chicago and Kansas City in 2003, and we have announced plans to establish five new RCFLs this year and three more in the near future, bringing the total number of FBI-sponsored RCFLs to 14.

The Intelligence Community

We have established much stronger working relationships with the CIA and other members of the Intelligence Community. From the Director's daily meetings with the Director of Central Intelligence and CIA briefers, to our regular exchange of personnel among agencies, to our joint efforts in specific investigations and in the Terrorist Threat Integration Center, the Terrorist Screening Center, and other multiagency entities, the FBI and its partners in the Intelligence Community are now integrated at virtually every level of our operations.

Terrorist Threat Integration Center

The Terrorist Threat Integration Center is a good example of our collaborative relationship with the CIA and other federal partners. Established on May 1, 2003, at the direction of President Bush, TTIC coordinates strategic analysis of threats based on intelligence from the FBI, CIA,

DHS, and DOD. Analysts from each agency work side-by-side in one location to piece together the big picture of threats to the U.S. and our interests. Each day *(except Sunday)*, TTIC analysts synthesize government-wide information regarding current terrorist threats and produce the Presidential Terrorism Threat Report for the President. The FBI personnel at TTIC are part of the Office of Intelligence and work closely with analysts at Headquarters. If TTIC sees a gap in the intelligence it receives, it notifies analysts at Headquarters, who in turn develop appropriate collection taskings and pass them to appropriate FIGs for execution.

Exchange of Personnel

The FBI currently has 34 people detailed to CIA entities, including 16 in the CIA's Counter Terrorism Center. We also have FBI agents and intelligence analysts detailed to the NSA, the National Security Council, DIA, the Defense Logistics Agency, DOD's Northern Command, and the Department of Energy.

CIA personnel are working in key positions throughout the Bureau. The Associate Deputy Assistant Director for Operations in the Counterterrorism Division is a CIA detailee. Four CIA officers are detailed to the Security Division, including the Assistant Director, the Chief of the Personnel Security Section, and managers working with the SCI program and the FBI Police. An experienced manager from the CIA's Directorate of Science and Technology now heads the Investigative Technologies Division, and a Section Chief in that division is on rotation from CIA.

This exchange of personnel is taking place in our field offices as well. In 33 field locations, the CIA has officers co-located with FBI agents at JTTF sites, and there are plans to add CIA officers to several additional sites. The NSA has analysts detailed to FBI Headquarters, the Washington Field Office, the New York Field Office, and the Baltimore Field Office.

Joint Briefings

Each morning, the Director is briefed by a CIA briefer. The Director of Central Intelligence and the FBI Director jointly brief the President on current terrorism threats. In addition, CIA and DHS personnel attend the Director's internal terrorism briefings every weekday morning and afternoon.

Secure Networks

The FBI is now using secure systems to disseminate classified intelligence reports and analytical products to the Intelligence Community and other federal agencies. The FBI hosts a web site on the Top-Secret Intelink/Joint World-Wide Intelligence Community System *(JWICS)*, a fully-encrypted system that connects more than 100 Department of Defense, CIA, and other Intelligence Community sites. We also host a web site on SIPRNET, a similar system used by DOD for sharing information classified at the Secret level. In addition, a new TS/SCI network known as "SCION" is being piloted in several field offices. SCION will connect FBI Headquarters and field offices to the CIA and other members of the Intelligence Community, and will increase opportunities for inter-agency collaboration.

Compatibility of Information Technology Systems

Improving the compatibility of information technology systems throughout the Intelligence Community will increase the speed and ease of information sharing and collaboration. Accordingly, the FBI's information technology team has worked closely with the Chief Information Officers *(CIOs)* of DHS and other Intelligence Community agencies, as we developed our recent and ongoing technology upgrades. This coordination has affected our decisions

on several key technology upgrades. For example, we chose an Oracle 9i Relational Database, in part, because this is the system used by the CIA.

To facilitate further coordination, the FBI CIO sits on the Intelligence Community CIO Executive Council. The Council develops and recommends technical requirements, policies and procedures, and coordinates initiatives to improve the interoperability of information technology systems within the Intelligence Community. It was established by Director of Central Intelligence directive and is chaired by the CIA's CIO.

Terrorist Explosive Device Analytical Center

According to a recent State Department report, more than 85 percent of all terrorist attacks against U.S. citizens and interests during the past five years involved improvised explosive devices *(IEDs)*, otherwise known as homemade bombs. Unlike manufactured military ordnance, these bombs often reflect the unique characteristics, or signature, of the terrorist organizations or individuals who made them. A systematic examination of IEDs can help the Intelligence Community draw linkages between terrorist devices and the individuals involved in their construction, and thereby improve our chances of preventing a terrorist attack. Until recently, there was no single federal agency responsible for the worldwide collection, complete forensic analysis, and timely dissemination of intelligence about terrorist IEDs.

In December 2003, the FBI Laboratory began preliminary operations of the Terrorist Explosive Device Analytical Center *(TEDAC)* to coordinate and manage a unified national effort to gather and exploit information on IEDs recovered both inside and outside the U.S. While the FBI manages the TEDAC, the CIA, DIA, NSA, and the Bureau of Alcohol, Tobacco, Firearms and Explosives all contribute to its intelligence efforts.

TEDAC has several functions. It collects unexploded IEDs, post blast debris, and bomb making material recovered from bombing scenes and suspected terrorist caches from all over the world. TEDAC personnel thoroughly examine this material to gather as much information as possible regarding its design and components and any forensic evidence of the builder, such as fingerprints, hairs, or DNA. TEDAC then analyzes and shares that information with domestic law enforcement authorities, intelligence and homeland security agencies, and foreign law enforcement and intelligence service counterparts. TEDAC also uses the knowledge gained from its examinations and analysis to assist in the investigation of terrorist bombing attacks, to develop new countermeasures to defeat IEDs, and to train first responders on terrorist IED techniques.

Department of Homeland Security

DHS plays a critical role in assessing and protecting vulnerabilities in our national infrastructure and at our borders, and in overseeing our response capabilities. We have worked closely with DHS to ensure that we have the integration and comprehensive information sharing between our agencies that are vital to the success of our missions. The FBI and DHS share database access at the TTIC, in the National JTTF at FBI Headquarters, in the FTTTF and the TSC, and in local JTTFs in our field offices around the country. We worked closely together to get the new Terrorist Screening Center up and running. We hold weekly briefings in which our CTD analysts brief their DHS counterparts on current terrorism developments. We coordinate all FBI warnings with DHS,

and we now coordinate joint warnings through the Homeland Security Advisory System to address our customers' concerns about multiple and duplicative warnings. We designated an experienced executive from the Transportation Security Administration to run the TSC and detailed a senior DHS executive to the FBI's Office of Intelligence to ensure coordination and transparency between the agencies.

On March 4, 2003, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence signed a comprehensive Memorandum of Understanding *(MOU)* establishing policies and procedures for information sharing, handling, and use. Pursuant to that MOU, information related to terrorist threats and vulnerabilities is provided to DHS automatically without DHS having to request it. Consistent with the protection of sensitive sources and methods and the protection of privacy rights, we now share as a rule, and withhold by exception.

Foreign Governments

With terrorists traveling, communicating, and planning attacks all around the world, coordination with our foreign partners has become more critical than ever before. We have steadily increased our overseas presence since September 11, 2001, and now routinely deploy agents and crime scene experts to assist in the investigation of overseas attacks, such as the May 2003 bombings in Saudi Arabia and Morocco. As of January 7, 2004, 413 FBI personnel were assigned overseas, over 200 of whom are permanently assigned. Their efforts, and the relationships that grow from them, have played a critical role in the successful international operations we have conducted over the past 31 months.

International Investigations

Bureau personnel have participated in numerous investigations of terrorist attacks in foreign countries over the past 31 months. Our approach to those investigations differs from the approach we traditionally have taken. Prior to September 11, 2001, our overseas investigations primarily were focused on building cases for prosecution in the U.S. Today, our focus is more broadly to provide our foreign partners with investigative, forensics, or whatever type of support will enhance our joint efforts to prevent and disrupt terrorist attacks. Our partners have embraced this approach, and it is paying dividends with greater reciprocal cooperation and more effective joint investigations.

By way of an example, our Legal Attaché office in Islamabad, Pakistan, was extensively involved in the investigation of the abduction and murder of *Wall Street Journal* reporter Daniel Pearl. The FBI conducted a forensic examination of a lap top computer seized by the Pakistani police that revealed a draft of the demand note for Pearl's release. FBI agents later returned to Pakistan and testified in the trial of Omar Sheikh and his co-conspirators, resulting in their convictions and a capital sentence for Sheikh.

Expansion of Legal Attaché Offices

Director Freeh recognized the need for greater operational collaboration with foreign government services, and during his tenure the FBI expanded the number of Legal Attaché offices from 23 to 44. Since September 2001, we have opened three more Legal Attaché offices, in Beijing, China, Abu Dhabi, United Arab Emirates, and Sanaa, Yemen. We plan to open an office in Kuala Lumpur, Malaysia, with the arrival of the Legal Attaché in May 2004. Construction and certification of our office in Tbilisi, Georgia, will soon be complete, and the office will open with the arrival of our Legal Attaché in June 2004. We also expect to open an office in the new U.S. Embassy building in Sofia, Bulgaria, this fall. We have gained Congressional approval and appropriations for offices that are currently in the design or construction bidding phases

in Rabat, Morocco, and Jakarta, Indonesia, and we expect to be in the design phase for a new office in Sarajevo, Bosnia, in April 2004. We are also in the design phase for sub-offices in Bonn, Germany, and Milan, Italy.

Joint Task Forces and Operations

The FBI is working with its international partners in new ways, including task forces, new information sharing initiatives and, in some cases, joint operations.

The following are a few examples:

U.S. / Saudi Joint Task Force on Terrorist Financing – On August 31, 2003, the FBI, other federal agencies, and the Saudi Mabahith formed an unprecedented task force to identify persons or entities suspected of providing financial support to terrorist groups overseas and to develop strategies to stem the tide of such support. Personnel from the FBI's Terrorist Financing Operations Section have been sent to Saudi Arabia to participate.

Riyadh "Fusion Cell" – The bombings of three western residential compounds on May 12, 2003, prompted a new and much improved level of cooperation between the FBI's Legal Attaché in Riyadh, other elements of the U.S. government represented in Riyadh, and the Saudi government. In May 2003, a team deployed from FBI Headquarters, in concert with our Legal Attaché in Riyadh, agreed to work jointly in investigating the attacks and the threat to the U.S. emanating from al-Qa'ida members in the Arabian Peninsula.

The result was a "fusion cell" that gave the Saudi government a single point of contact for U.S. elements assisting in the investigation. The fusion cell coordinates requests for information, concentrates resources for interviews and debriefings, and serves as a coordination point for information from all sources.

Indonesian Joint Operation – The FBI's Counterterrorism Division, in conjunction with the New York and Los Angeles Divisions, has deployed personnel to Indonesia since October 2002 as part of an initiative with the Indonesian National Police and the Australian Federal Police to investigate the October 12, 2002, Bali bombings and the August 5, 2003, J.W. Marriott Hotel Bombing. The FBI participates in regular coordination meetings with both agencies, and we are lending extensive investigative support to the initiative, including technical assistance, laboratory testing, and forensic support.

Fingerprint/Identification Initiatives

Critical to our counterterrorism efforts is the use of biometric and biographical information to establish a person's identity conclusively. Several new initiatives are helping us expand our intelligence base with critical identifiers, such as fingerprints, DNA, photographs, and biographical information from foreign sources. The FBI's Criminal Justice Information Services Division has led several overseas deployments to gather and exchange fingerprints of known and suspected terrorists. CJIS has obtained fingerprints and other identifying information for more than 10,000 terrorist suspects and detainees from more than 16 countries. DOD and CJIS are adding selected enemy combatant fingerprints to existing fingerprint databases and making them available for military, law enforcement, and homeland security needs. CJIS is also working closely with DOD, the Navy, Army, and Marine Corps to provide identification services and assistance in Iraq and Afghanistan. Lastly, CJIS personnel have provided basic training to foreign law enforcement entities on how to take viable and legible fingerprints that can be used reliably by the FBI and our partners.

International Training Initiatives

We are increasing training opportunities for our foreign partners at the FBI National Academy and at the International Law Enforcement Academies *(ILEAs)* in Hungary and Thailand. Since September 11, 2001, the Bureau has trained over 20,000 international law enforcement students on topics ranging from management principles to law enforcement communications to forensic science. In addition, we have several new initiatives:

- At the request of the Coalition Provisional Authority in Iraq, FBI, DHS, State Department, and other DOJ personnel traveled to Baghdad, met with law enforcement and Coalition Provisional Authority officials, assessed their needs, and developed a comprehensive training plan. The plan includes training in counterterrorism and post-blast investigations, major case management, fingerprinting, organized crime investigations, and the development of an internal affairs apparatus. The plan is awaiting approval by the Coalition Provisional Authority.
- The Middle Eastern Law Enforcement Training Center *(MELETC)*, located at the Dubai National Police Training Academy in Dubai, United Arab Emirates, is a bilateral partnership between the Government of the Emirate of Dubai and the FBI. Through the MELETC, the FBI provides training and assistance in counterterrorism and other disciplines to officers from the Dubai National Police and other Gulf Cooperation Council *(GCC)* countries. To date, over 400 police officials from the GCC have received training at MELETC.
- In a new program funded by the State Department, experts from our Terrorist Financing Operations Section and the Internal Revenue Service offer a course on terrorist financing and money laundering for foreign law enforcement officers and banking regulators. The course has been offered to officials from 10 countries since February 2003, and training is planned for eight additional countries in 2004.
- The Cyber Division conducted 12 specialized courses outside the U.S. *(involving almost 500 students)* this past year to raise the expertise and analytical abilities of foreign personnel involved in investigating computer intrusions and cyber crime matters.
- The FBI-supported forensic training laboratory in the ILEA in Budapest opened in January 2004. The FBI provided laboratory equipment for this new training center, and FBI Laboratory experts serve as instructors. The center will help raise the overall level of forensic expertise in Eastern and Central Europe and Central Asia as students return to their home countries to combat crime and terrorism.
- The FBI's Training and Development Division is spearheading "Leadership in the Counterterrorism Environment," an international training initiative for certain North American and United Kingdom law enforcement agencies. The program is focused on developing and refining strategic leadership skills for intelligence and counterterrorism missions. Training is tentatively scheduled for sites in Scotland and Northern Ireland this summer, and at the FBI Academy this fall.

The relationships fostered by these training initiatives have borne fruit in improved operational coordination. In the aftermath of the May 2003 bombings in Riyadh, Saudi Arabia that killed nine Americans, we received unprecedented cooperation from Saudi officials. One reason was the fact that the FBI National Academy had recently trained more than 100 Saudi police in the science of evidence collection. As a result, our forensic technicians and their Saudi

counterparts were using the same terminology and methods of evidence collection. As our Saudi partners told us, “We were taught together, now we can work together.”

The Private Sector

The FBI increasingly looks to partnerships with the private sector to enlist support for its law enforcement and intelligence missions. Among those partnerships are the following:

Community Outreach

If the FBI is successfully to predict and prevent terrorist attacks, it is imperative that we build and maintain close ties to key minority communities. The Muslim, Iraqi, and Arab-American communities have contributed a great deal to our successes to date, and we are grateful for their assistance and for their ongoing commitment to preventing acts of terrorism.

Beginning in late 2001, Director Mueller has met bi-annually with a group of leaders from the Arab American, Muslim American, and Sikh American communities to discuss issues including counterterrorism efforts, terrorism-related money transactions, "no-fly" lists, training on cultural awareness, and recruiting. In addition, each FBI field office was tasked with establishing contacts with Arab-American, Muslim, and Sikh community organizations and leaders in their territories. Since September 11, 2001, high-level field managers have attended over 1,880 town hall, community, or association meetings; participated in over 900 meetings with Muslim, Sikh, or Jewish groups; and attended over 300 meetings with civil rights leaders to address their concerns. Field managers also sponsored over 130 sessions of training by representatives of Middle Eastern groups in order to improve our agents’ cultural awareness and sensitivity.

These efforts to reach out to Muslim and Arab American communities assist our counterterrorism efforts by improving the level of cooperation and the number of tips received from these communities. Outreach efforts also support long-term recruitment goals and the overall public understanding of terrorism.

InfraGard

InfraGard is a partnership between the FBI and the private sector designed to foster the exchange of information between law enforcement and the owners and operators of our nation's critical infrastructure. Using a secure web site, InfraGard members receive sensitive, but unclassified, information such as Alerts, Advisories and Information Bulletins from the FBI and DHS. In turn, members provide information relevant to FBI investigations.

InfraGard currently has 10,000 members and 79 chapters throughout the 56 field divisions. These members primarily represent small and medium-sized businesses in all of the critical infrastructure sectors. Over the past year InfraGard membership increased by 44 percent.

InfraGard chapters meet regularly to discuss cyber crime, terrorism, and criminal threats to critical infrastructures, and often include representatives from state, municipal and federal government, academia, and law enforcement agencies. At a time when the failure to report cyber crimes remains a major obstacle to stopping these crimes, InfraGard helps us build trust and encourages reporting. The program allows us to alert companies to threats so they can better protect themselves, and ultimately helps us identify and counter those groups and individuals who threaten our critical infrastructures.

Financial Sector Outreach

Expanding upon long established relationships between the FBI's white-collar crime program and the financial services industry, the Terrorist Financing Operations Section conducts extensive liaison with the financial community through a series of national and international initiatives – including the training efforts referenced above. In addition, in spring of 2003, we established Special Agent Terrorism Financing Coordinators in each JTTF to share information and improve relationships with financial institutions in their areas.

Railroad Initiative

As evidenced by the recent bombings in Madrid, Spain, America's rail companies have significant critical assets that, if compromised, could cause a serious disruption to our national infrastructure. To enhance our liaison with this critical sector, we invited a railroad police officer, who represents the nation's railroad police, to join our National Joint Terrorism Task Force. In August 2003, a Supervisory Special Agent from the Norfolk Southern Railroad Police Department reported to the NJTTF. Working through this representative, we now provide training to JTTFs that have critical railroad assets in their areas, familiarizing them with those assets and the various measures for their protection.

INFORMATION TECHNOLOGY

The foundation of a centralized and effective counterterrorism operation is the capability to assemble, assimilate, and disseminate investigative and operational information both internally and with fellow intelligence and law enforcement agencies. This capability requires information technology *(IT)* that makes information easily accessible and usable by all personnel while protecting the security of that information.

On September 11, 2001, the Bureau's information technology was inadequate to support its counterterrorism mission. In preceding years, substantial investments were made to upgrade technologies that directly supported investigations, such as surveillance equipment and forensic services like the Integrated Automated Fingerprint Identification System. Insufficient attention was paid, however, to technology related to the more fundamental tasks of records creation, maintenance, dissemination, and retrieval. In 2001, many employees still used vintage 1987 386 desktop computers. Some resident agencies could only access data in their field office via a slow dial-up connection. Many Bureau programs were using computer systems that operated independently and did not interoperate with systems in other programs or other parts of the Bureau.

We also had a deficient information management system. The FBI's legacy investigative information system, the Automated Case Support *(ACS),* was not very effective in identifying information or supporting investigations. Users navigated with the function keys instead of the "point and click" method common to web-based applications. Simple tasks, such as storing an electronic version of a document, required a user to perform 12 separate functions in a "green screen" environment. Also, the system lacked multimedia functionality to allow for the storage of information in its original form. Agents could not store many forms of digital evidence in an electronic format, instead having to describe the evidence and indicate where the evidence was stored in a control room.

Thanks to the character and resolve of its personnel, the FBI was able to achieve numerous investigative successes, in spite of these obstacles. It was clear as of September 11, 2001, however, that we needed an integrated IT infrastructure to manage our information. We brought on-board a highly skilled team of experts and set out to create an IT infrastructure that is fast and secure, and that ties together the applications and databases used throughout the Bureau. We also designed user-friendly, web-based software applications to reduce reliance on paper records and to streamline investigative workflow. These improvements are enhancing our ability to collect, store, search, analyze, and share information.

Centralized Management

The shortcomings of the FBI's IT prior to September 11, 2001, were due in part to a lack of centralized management. Decisions related to IT were made at various levels and by various divisions throughout the Bureau with no overarching strategy or plan. To correct this problem and ensure that future decisions related to IT are consistent with a clear plan to meet

FBI-wide needs, we have centralized decision-making related to IT. In July 2002, the Director appointed the first full-time Chief Information Office *(CIO)* for the FBI. The CIO is responsible for the FBI's overall information technology efforts, including: **1**) developing our IT strategic plan and operating budget; **2**) developing and maintaining the FBI's technology assets; and **3**) providing technical direction for the re-engineering of FBI business processes. In December 2003, Director Mueller appointed a Chief Technology Officer who is responsible for guiding the information technology research and development functions of the FBI. He is currently focused on centralizing our current IT development projects, ensuring the optimal use and sharing of Bureau intelligence data on common platforms. We also created an Enterprise Architecture Board made up of 14 representatives from eight FBI divisions. The Board meets regularly to review technical proposals for new FBI information systems.

Trilogy

The first step in our modernization efforts is the Trilogy Program, a multi-year effort to enhance our effectiveness through technologies that allow us better to access, organize, and analyze information. The Trilogy Program is aimed at providing all FBI offices, including Legal Attaché offices, with improved network communications, a common and current set of office automation tools, and user-friendly web-based applications. Trilogy upgrades also incorporate controls to provide an enhanced level of security for FBI information. Trilogy has proceeded in three stages or components:

1 Transportation Network Component

We replaced old local area and wide area networks with a state-of-the-art, secure, high-speed communications system that links desktops and databases throughout the FBI. This component was completed on March 28, 2003, with deployment of a new wide area network to 591 sites, 622 local area networks, and 1,202 local area network switches. We launched a highly secure network connected to the nation's Intelligence Community in order to facilitate the transmission and sharing of Top Secret *(TS)* and Sensitive Compartmented Information *(SCI)*. We also created an Enterprise Operations Center to manage data, the network, hardware, software applications, and security access.

2 Information Presentation Component

We upgraded antiquated computers with new desktops, fast black and white and color printers, scanners, new office automation software and e-mail, and modern server technology for data storage and sharing. Employees now work with modern desktops and connectivity, facilitating their ability to input, retrieve, manipulate, and present information in text, image, audio, and video formats. To date, we have deployed 29,889 new desktop computers, over 7,500 upgraded desktop computers, 3,689 printers, 1,580 scanners, 465 servers and 1,382 routers.

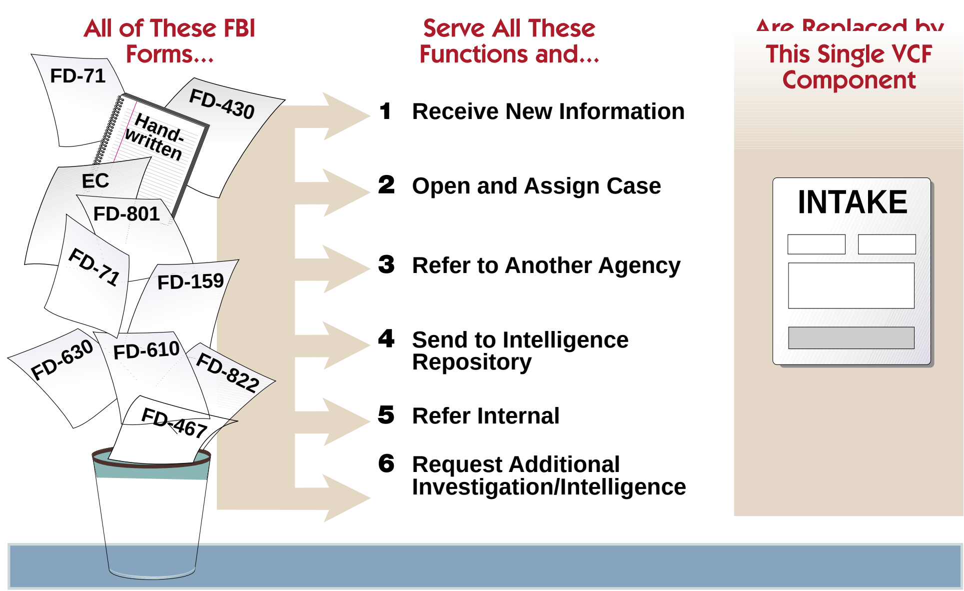
3 User Application Component—The Virtual Case File

The final component is the complete replacement of the outdated investigative information system, the Automated Case Support System. As an intermediate fix, we created a more user-friendly, web-based interface for ACS. This interface significantly reduces the number of keystrokes needed to perform routine functions, allows users to search multiple databases within ACS simultaneously, and eliminates the need to convert documents to a new format prior to uploading.

We then designed, and are now working to implement, a completely new system, known as the Virtual Case File *(VCF)*. VCF is a web-based information and case management tool that will re-engineer the FBI's workflow and significantly enhance the analytical capabilities of each Special Agent and analyst. The VCF will be a "point and click," "drag and drop" environment with the ability to access cases, leads, and evidence from the desktop. The VCF represents a revolutionary shift away from paper case files to digital files that can quickly be accessed by agents, analysts, and supervisors throughout the Bureau. Agents investigating a complex case will be able to view evidence and documents related to the investigation instantly, regardless if they are in different offices or even different countries. The VCF will allow for quicker, smoother collaboration across the organization, and will also simplify information sharing with outside partners. At the same time, VCF will enhance security by making it easier to control and monitor who has access to the system and its information.

The VCF will replace numerous forms and the multi-step functions of ACS with simple web-based processes. As depicted in the following diagram, for example, the VCF's single "Intake" function will allow agents or their supervisors to perform numerous functions – receive new information, open and assign a case, refer items to another agency, send intelligence to a central location, or request additional investigation to gather intelligence.

VCF Business Process Re-Engineering Example: INTAKE



Deployment of the VCF was originally scheduled for December 2003, but has been delayed due to a failure on the part of a contractor to complete certain engineering tasks by October 2003, as specified in their contract. We have renegotiated the contract, and we now expect to have VCF tested and deployed later this year. We are using the interim to continue our training efforts, so that FBI personnel are ready to hit the ground running when VCF comes online.

Data Warehousing

Following the attacks of September 11, 2001, we saw the need to provide counterterrorism investigators and analysts with quick, easy access to the full breadth of information relating to terrorism. We developed a three-step plan that would provide immediate support to

counterterrorism investigators and analysts, and then incrementally increase the range and effectiveness of that support for other criminal investigations. This plan transitions us away from separate systems containing separate data *(ACS, TelApps)* towards an Investigative Database Warehouse *(IDW)* that contains all data that can legally be stored together. The IDW provides the Bureau with a single access point to several data sources that were previously available only through separate, stove-piped systems. By providing consolidated access to the data, for the first time analytical tools can be used across data sources to provide a more complete view of the information possessed by the Bureau.

1 SCOPE

The initial step toward the IDW was the implementation of the Secure Counterterrorist Operational Prototype Environment *(SCOPE*) program. Under the SCOPE program we quickly consolidated counterterrorism information from various data sources, providing analysts at Headquarters with substantially greater access to more information in far less time than with other FBI investigative systems. The SCOPE database also gave us an opportunity to test new capabilities in a controlled environment. This prototype environment has now been replaced by the IDW.

2 Investigative Data Warehouse

The IDW, delivered in its first phase to the Office of Intelligence in January 2004, now provides analysts with full access to investigative information within FBI files, including ACS and VGTOF data, open source news feeds, and the files of other federal agencies such as DHS. The IDW provides physical storage for data and allows users to access that data without needing to know its physical location or format. The data in the IDW is at the Secret level, and the addition of TS/SCI level data is in the planning stages.

Later this year, we plan to enhance the IDW by adding additional data sources, such as Suspicious Activity Reports, and by making it easier to search. When the IDW is complete, agents and analysts using new analytical tools will be able to search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. They will be able to extract subjects' addresses, phone numbers, and other data in seconds, rather than searching for it manually. They will have the ability to identify relationships across cases. They will be able to search up to 100 million pages of international terrorism-related documents in seconds.

3 Master Data Warehouse

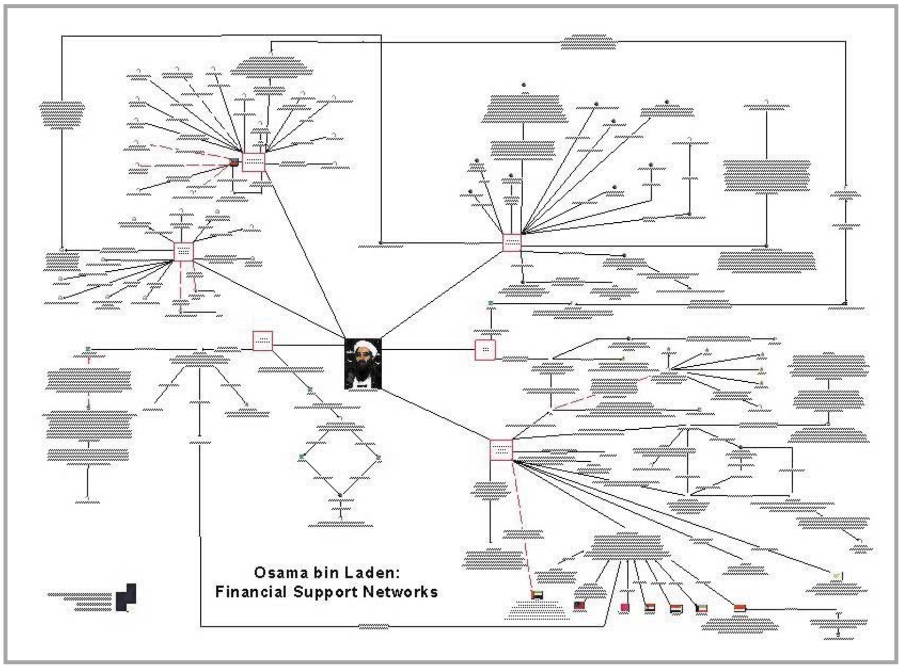
Ultimately, we plan to turn the IDW into a Master Data Warehouse *(MDW)* that will include the administrative data required by the FBI to manage its internal business processes in addition to the investigative data. MDW will grow to eventually provide physical data storage for, and become the system of record for, all FBI electronic files.

Analytical Tools

We are introducing advanced analytical tools to help us make the most of the data stored in the IDW. These tools allow FBI agents and analysts to look across multiple cases and multiple data sources to identify relationships and other pieces of information that were not readily

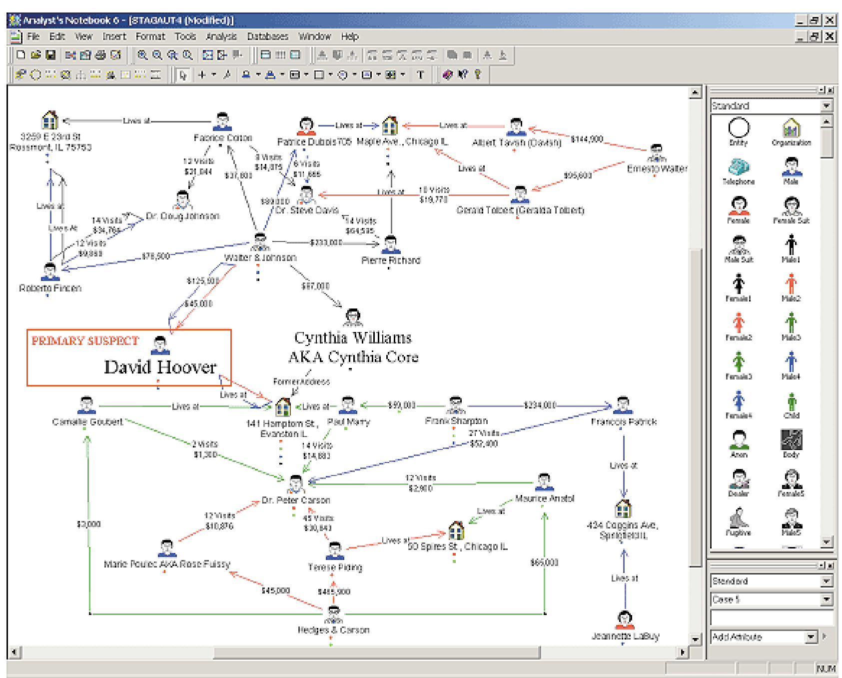
available using older FBI systems. These tools **1)** make database searches simple and effective; **2)** give analysts new visualization, geomapping, link-charting and reporting capabilities; and **3)** allow analysts to request automatic updates to their query results whenever new, relevant data is downloaded into the database.

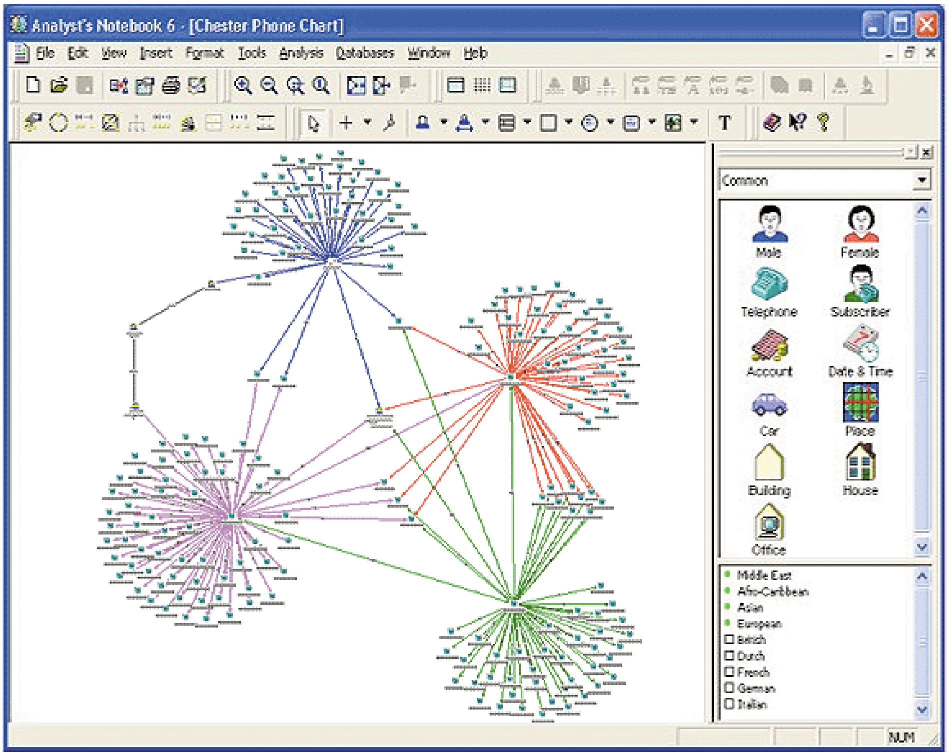
The following are fictional examples that illustrate how some of these tools can assist analysts in drawing connections between discrete pieces of information:



Analysts can create high-level diagrams showing linkages between organizations to reveal front organizations suspected of being involved in terrorist financing.

Analysts can diagram the relationships between people, locations, and money transfers.





They can also depict different groupings of individuals to establish which individuals are common to multiple groups.

Putting it all together

As the first part of our IT modernization efforts nears completion, FBI agents, analysts, and support personnel are already enjoying new capabilities and applying those capabilities to their counterterrorism mission. They have up-to-date desktops, fast and secure connectivity, a user-friendly interface to the ACS case management system, the ability to access and search consolidated terrorism-related data, and new capabilities for sharing information inside and outside the Bureau.

In the coming year, the Virtual Case File will revolutionize work processes related to case and information management. It will be easier than ever to resolve leads, find connections, and ensure that information finds its way to the agents, analysts, and managers who need to see it in real time.

While there is still much to be done, these efforts are starting to deliver the technology we need to stay ahead of evolving threats. Upgrading our technology will remain an FBI priority for the foreseeable future, and our new IT management will ensure that we continue to improve our systems.

ADMINISTRATIVE REFORM

We realized at the outset that our plan for developing a strong counterterrorism capability would succeed only if we also develop the infrastructure and the administrative functions to support that operation. Without strategic planning, we cannot direct the distribution of resources necessary for our operations. Without a streamlined recruiting and hiring process, we cannot staff our new counterterrorism units. Without modern records management, we cannot make full use of our technology upgrades, and without a comprehensive security apparatus, we cannot adequately assure the integrity of sensitive investigative information and operational plans.

Recognizing that the business and administrative practices in place on September 11, 2001, were not adequate to support our counterterrorism mission, we initiated an effort to re-engineer our administrative infrastructure. We undertook a series of re-engineering projects that address discrete areas of our operations. These reforms – some now fully developed and some still in progress – are making the Bureau more administratively nimble and responsive to operational needs.

Strategic Planning

We have reworked the FBI's strategic planning process. We have produced – and are currently revising with input from the General Accounting Office – a five-year Strategic Plan that will guide our executive management decisions. The FBI's Strategic Plan provides clear goals and objectives, but also has the flexibility necessary to allow us to adjust quickly to evolving threats. The strategic planning process translates these goals and objectives into actionable and measurable activities in order to track our progress. Annual implementation plans provide performance goals and measures to incrementally achieve the FBI's strategic goals, and completion dates are assigned and tracked to ensure deadlines are met. Comprehensive program evaluations are conducted to measure whether we have met the performance goals and objectives set forth in the Strategic Plan.

As our Intelligence Program continues to mature, we expect our strategic planning to become increasingly sophisticated. We will rely on our intelligence base to develop a comprehensive assessment of future national security and criminal threats. Then, we will use it to develop short and long-term proactive strategies to deal with each threat, to determine how our operations and capabilities must change, and to calculate how we should manage, deploy, and acquire new resources to counter those threats.

Realigning the Workforce

The FBI's greatest strength is its people, and their investigative and analytical skills remain our greatest weapons in the fight against terrorism. If the FBI's transformation is to succeed,

however, we need to continue developing a workforce with critical skills and the experience and flexibility to adapt quickly to changing priorities. Accordingly, we have made a number of changes to the way we recruit, hire, train, and promote our personnel – changes which are in addition to the recent personnel initiatives *(discussed above)* that focus specifically on intelligence capabilities. These new efforts to realign our workforce will help ensure that the FBI is ready to address evolving threats well into the future.

Revised Personnel Selection Process

In the years prior to September 11, 2001, Special Agent hiring efforts focused primarily on individuals with law enforcement, military, accounting, and legal backgrounds. For example, of the 285 agents hired in 2001, 19 had law degrees, 15 had a background in accounting, 26 had language skills *(mostly Spanish to assist with narcotics trafficking investigations)*, and the remainder were primarily from law enforcement or military backgrounds. This hiring approach produced tremendous investigators, whose efforts and dedication have been the building blocks of the FBI's reputation for excellence.

Now that the FBI's mission and the threats we face are changing, there is a new need for certain specialized skills, such as intelligence, engineering and language capabilities. While we continue to draw from traditional sources in our hiring, we are augmenting our recruitment efforts and personnel selection process to ensure that we hire more individuals with the specific skills and experience that match our priorities and overall intelligence efforts. We devised a new recruitment strategy that includes: **1)** initiating a major marketing campaign; **2)** recruiting at colleges and universities with outstanding programs in critical skills areas; **3)** partnering with the U.S. Copts Association to recruit individuals with Arabic language skills; **4)** changing the FBI's web site to focus on job opportunities in the intelligence and counterterrorism fields; and **5)** modifying the Presidential Management Fellows Program and the Honors Internship Program to recruit only candidates who possess critical skills.

In February 2003, SACs were given guidance and instruction on leading targeted recruitment efforts. Since that time, the SACs have been evaluated on their recruitment efforts on a quarterly basis.

We also revised the hiring process itself by changing the list of critical skills we are looking for in candidates to include: intelligence background *(including experience in the Intelligence Community or significant expertise in international studies)*; languages helpful to our counterterrorism and/or counterintelligence missions; information technology and computer science; engineering; physical sciences; accounting; and international business. We similarly changed the screening criteria on which candidates for Special Agent positions are evaluated at each stage of the hiring process. The result has been a significant increase in the number of new Special Agents with expertise in these areas.

Special Agents hired with critical skills

Critical Skills:	2002	2003
Intelligence experience/expertise	65	123
Computer Science/IT	66	171
Physical/Life Sciences	72	105
Engineering	68	82
Foreign Languages	48	72

Streamlined Hiring Process

The FBI has historically had an overly lengthy and cumbersome hiring process that has impeded our ability to bring on the personnel to meet emerging threats and needs. Thanks to a concerted effort by the Administrative Services Division, the average time for the background investigation process has been reduced from over six months to less than three months, which has helped us hire significantly more support personnel. We hired a total of 1,145 support employees in 2003 *(including over 200 analysts)* compared to a total of 365 in 2002.

To improve efficiency further, we purchased new software to automate the hiring process, and plans are in the works for a Centralized Processing Center that will house all major functions related to processing applications for certain positions in the FBI. Having functions such as testing, personnel security interviews and polygraphs in the same facility will keep the hiring process consistent, help us keep applicants informed of progress, and create efficiencies to move successful applicants quickly into the background check process.

Training

Traditionally, the FBI's Training Division focused on two flagship programs based at the FBI Academy in Quantico, Virginia – training for new Special Agents and the National Academy for non-FBI law enforcement officers. For a variety of reasons, including inadequate resources and fragmented training responsibilities, limited progress was made in support of career development for on-board employees.

To address this issue, we significantly expanded the resources and responsibilities dedicated to workforce training, and we instituted a new training management structure. We replaced the old Training Division with the more expansive Training and Development Division, and we are in the process of recruiting an Assistant Director who will be responsible for the development and distribution of training for all FBI employees. The Assistant Director will be supported by a new staff of training professionals in the Office of Training Development *(OTD)* at Headquarters, a Special Agent in Charge who will manage day-to-day operations at the FBI Academy, and a Senior Executive Service-level Dean of Academics who will focus on developmental training for on-board employees.

Executive Leadership Initiatives

The FBI has an extremely talented cadre of supervisors both in the field and at Headquarters. To keep this cadre as strong as possible, we have launched several new initiatives. These efforts help our leaders manage changes related to the FBI's transformation, and ensure that managers have the broad range of experience and flexibility needed to adapt quickly to changing priorities.

Leadership Skills Assessment (LSA) – As part of our efforts to develop senior managers and prepare individuals with high potential for executive leadership roles, we instituted a new Leadership Skills Assessment for all employees interested in pursuing supervisory positions within the Bureau. The LSA is a live telephonic role simulation in which candidates play the role of either a squad supervisor or an ASAC, and it evaluates eight core competencies determined to be essential for successful performance as a mid-level manager in the FBI.

These core competencies are: Leadership, Interpersonal Ability, Liaison, Organizing and Planning, Problem Solving/Judgment, Flexibility/Adaptability, Initiative, and Communications.

Management Training – Our Senior Executive Service personnel are going through an executive development program that was created in partnership with the Kellogg School of Management, one of the country's leading business schools. In an intensive one-week course, FBI executives receive guidance on managing change, with a particular focus on the FBI's transition to new intelligence, investigative, and case management processes. As of February 13, 2004, 260 FBI executive managers have completed the training, including 12 Assistant Directors and 54 SACs.

Records Management

In the spring of 2001, FBI personnel located over 3,000 Bureau records relating to the Timothy McVeigh investigation that had not been previously identified, collected, and disclosed to McVeigh's defense counsel. This oversight was not intentional; it was the result of a deficient system for the storage and cataloguing of our investigative records.

Records management is at the heart of the FBI's effectiveness and integrity as a law enforcement organization. The ability to maintain, access, and retrieve documents is critical to our investigative mission and is a fundamental element of our analytical capability. Over the past 31 months, we have taken significant steps to overhaul our FBI-wide records management capabilities, to increase accountability for compliance with established records procedures, and to train our employees about the advantages of a paperless environment.

Centralizing Records Management

On January 7, 2002, we created the Records Management Division *(RMD)* to direct and oversee all records policy and functions. RMD is headed by an Assistant Director who serves as the FBI's Records Officer. RMD consolidates all records operations to ensure consistency, thoroughness, and accountability.

As we evaluated our records management process, it became clear that a central location would improve general efficiency and facilitate compliance with National Archives and Records Administration *(NARA)* standards. We are finalizing plans to consolidate the RMD and all the files currently stored in 265 storage locations at one facility outside of FBI Headquarters. This facility will provide central management and storage for all active and inactive case files, allowing the field offices and FBI Headquarters to get out of the file storage business.

Turning Paper into Searchable Data

Until very recently, the Bureau used a records management system that relied primarily on the filing and retention of paper copies of investigative reports and other relevant documents. The FBI has made substantial progress moving from paper files to an electronic records system that Bureau personnel can access from their desktop computers. New documents and files are now routinely uploaded into our electronic case management system. We are also converting our legacy paper files by scanning documents to create digital images. The digital images are then converted into searchable digital text or tagged so they can be retrieved during searches.

New Records Control Schedule

In March 2004, we announced a new proposed records control schedule for FBI investigative, analytical, and administrative case files. The control schedule is the legal authority governing the length of time that FBI investigative and administrative case records are kept before they are destroyed or transferred to the NARA. The schedule was developed in partnership with NARA as part of their Targeted Assistance Program. The proposed schedule is subject to public notice and comment before it can be formally approved, and will soon be published in the *Federal Register*. The schedule is an important milestone in our efforts to modernize our records management process, replacing authorities that have been out of date for more than a dozen years.

Improving Efficiency

Re-engineering efforts are improving productivity and efficiency in our records management. For example, we established a Service Request Center to coordinate Freedom of Information Act and the Privacy Act *(FOIPA)* requests. The backlog of pending FOIPA requests has dropped 40 percent, from 2,650 in October 2002 to 1,600 today, and pending FOIPA appeals have dropped 67 percent, from 780 to 257. We also improved the efficiency of our Name Check Program. In late 2001, with new visa screening requirements, we were overwhelmed by the increase in names to be checked. To address the resulting backlog, we developed and implemented an internal tracking system, modified our software to provide detailed metrics, and increased the personnel by 65 percent. The backlog was all but eliminated.

Security Management

The FBI has built, and continues to improve, a comprehensive and centralized security program. On December 3, 2001, we created the Security Division headed by an Assistant Director. Since then, the Security Division has consolidated personnel security, physical security, and information security functions that were previously distributed across diverse FBI activities. The Division has put in place the following initiatives, among others:

Information Assurance Plan

The FBI developed a comprehensive information assurance plan, modeled on the best practices of the Intelligence Community, and considerably enhanced the security of its information systems. For example, the new Trilogy network provides a high level of security and new capabilities, such as the ability to track unauthorized access to files. A key part of this program is the involvement of security experts in the development of the FBI's IT infrastructure to ensure that information assurance is part of the FBI's IT architecture.

In summer of 2002, we created the Information Assurance Section within the Security Division. We have since tripled the size of its Accreditation Unit, which conducts security risk assessments of IT systems from the planning and procurement stages, through the operation and eventual de-commissioning of each system. IT systems are certified and accredited if they meet federal information security standards. In fall of 2001, only 20 of the FBI's IT systems were accredited. Today, more than 100 have been accredited, improving our security and facilitating information sharing with other federal agencies.

Enterprise Security Operations Center

The new Enterprise Security Operations Center *(ESOC)*, which began operations on October 22, 2003, is tasked with protecting FBI information systems from external attacks and insider misuse through techniques such as real time network monitoring, intrusion detection, and data auditing. The ESOC is operated by security analysts around the clock.

Audits and Reviews

To help deter and detect espionage activities, the FBI instituted a number of new audits and reviews. We expanded our polygraph program to include all employees who have access to highly sensitive information or who are heading to or returning from a permanent overseas assignment. We developed and are implementing a Financial Disclosure Program that will ultimately include all FBI employees and contractors with SCI access. We also enhanced reviews of reinvestigation results for employees with the most sensitive security access.

Security Officers

The FBI has taken steps to build a Bureau-wide force of full-time, career-track security professionals. An important part of the security career track will be the new full-time position of Chief Security Officer, who will serve as the senior security representative in each field office and in each Headquarters division. Security Officers report directly to their division head or SAC.

Security Education

The FBI is implementing a comprehensive security education, awareness, and training program. FBI employees routinely receive e-mail security updates, and an internal web site now provides regular guidance on security measures. All employees recently took a refresher course on security matters. Security training for new Special Agents has been increased, and an updated security briefing for new employees, task force personnel, and contract personnel is being developed.

Disaster Recovery Planning

Each field office and Headquarters division has developed a plan to ensure continuity of operations in the event of an emergency. Efforts have also been made to ensure that vital records are secure in such an event.

ASSESSMENT OF OUR PROGRESS

With the recent directives implementing the intelligence agent career track and the administrative reforms related to building an intelligence workforce, we have in place the essential structural elements of an intelligence-driven counterterrorism operation. The challenge now is to refine and continue to develop that operation – an effort that will require additional resources, continued attention by FBI leadership, and constant training of FBI personnel in intelligence processes and objectives.

While we have clearly made substantial progress over the past 31 months, it is difficult to come up with an exact measurement of the current effectiveness of our counterterrorism efforts. Besides citing the absence of successful attacks on the homeland since September 11, 2001, there is no single measure that completely captures the progress we have made. *There are several yardsticks, however, that demonstrate the effectiveness of the core functions of a Counterterrorism Program. These yardsticks include the following:*

- **Development of human assets**
- **Number of FISAs**
- **Number of intelligence reports generated**
- **Quality of daily briefings**
- **Effectiveness of counterterrorism operations**
- **Continued protection of civil liberties**

An application of these yardsticks demonstrates the progress we have achieved since September 11, 2001.

Development of Human Assets

The FBI has long recognized that human source information is one of the most important ways to investigate criminal activity. We have long-standing expertise in recruiting and using human sources, and we have used those skills to great effect across a wide range of investigative programs, including organized crime, drugs, public corruption, and white collar crime.

While we also have developed sources over the years in the Counterterrorism Program, the September 11, 2001, attacks highlighted the shortage of human intelligence reporting about al-Qa'ida both in the U.S. and abroad. With the U.S. government having relatively few assets who were able to penetrate and report on al-Qa'ida's plans, we were vulnerable to surprise attack.

The Bureau has placed a priority on developing human intelligence sources reporting on international terrorists. We have revised our training program, our personnel evaluation criteria, and our operational priorities to focus on source development. While we continue to grow this

capacity, we have already seen a marked increase in the number of human intelligence sources in the Counterterrorism Program. Between August 30, 2001, and September 30, 2003, the number of sources related to international terrorism increased by more than 60 percent, and the number of sources related to domestic terrorism increased by more than 39 percent.

One effort to develop operational intelligence and long-term sources was the Iraqi Interview Project. In three weeks during the spring of 2003, in anticipation of a possible military conflict in Iraq, the FBI, along with our law enforcement partners, conducted more than 10,000 voluntary interviews with U.S.-based Iraqis. Many of the persons we interviewed – who included engineers, scientists, and even former leaders in the Iraqi government – had fled Iraq in fear of its then dictator. They were contacted by the FBI because of their possible knowledge of the Iraqi leadership, Iraqi military facilities, and Iraq's potential involvement with terrorism.

These interviews netted significant intelligence and operational information. As a result of these interviews, approximately 250 reports were provided to the U.S. military to assist in locating weapons production and storage facilities, underground bunkers, fiber optic networks, and Iraqi detention and interrogation facilities. Department of Defense representatives have stated that the information was timely, excellent, relevant, and greatly assisted in bridging gaps in other intelligence.

The interviewers also asked all subjects to report any incidents where they faced hostilities or attacks because of their ethnic background. As a result of these interviews, 36 hate crime incidents were reported and referred to DOJ's Civil Rights Division.

> Since September 2002, the number of FBI sources reporting on Iraqi matters increased 270%

Number of FISAs

FISA coverage has increased significantly since September 11, 2001, reflecting both our increased focus on counterterrorism and counterintelligence investigations and improvement in the operation of the FISA process. From 2001 to 2003, the number of FISA applications filed annually with the Foreign Intelligence Surveillance Court increased by 85 percent. We have seen a similar increase in the use of the emergency FISA process that permits us to obtain immediate coverage in emergency situations. In 2002, for example, the Department of Justice obtained a total of 170 emergency FISA authorizations, which is more than three times the number of emergency FISAs we obtained in the 23 years between the 1978 enactment of FISA and September 11, 2001.

Number of Intelligence Products Generated

In the past year, the FBI produced more than 3,000 intelligence products, including “raw” reports, intelligence memoranda, in-depth strategic analysis assessments, special event threat assessments, and focused Presidential briefings. We also conducted numerous intelligence briefings to members of Congress, other government agencies, and the law enforcement and intelligence communities. These efforts mark a new beginning for the FBI's intelligence operation.

Prior to September 11, 2001, the FBI produced very few raw intelligence reports. In FY 2003, we produced and disseminated 2,425 Intelligence Information Reports containing raw intelligence derived from FBI investigations and intelligence collection. The majority contained intelligence related to international terrorism; the next greatest number contained foreign intelligence and counterintelligence information; and the remainder concerned criminal activities and cyber crime. These IIRs were disseminated to a wide customer set in FBI field offices, the Intelligence Community, Defense Community, other federal law enforcement agencies, and U.S. policy entities.

In addition to these individual reports, the FBI developed and issued in January 2003 a classified comprehensive assessment of the terrorist threat to the U.S. This assessment focuses on the threats that the FBI sees developing over the next two years, based on an analysis of information regarding the motivations, objectives, methods, and capabilities of existing terrorist groups and the potential for the emergence of new terrorist groups and threats throughout the world. This threat assessment is used as a guide in the allocation of investigative resources, as a useful compilation of threat information for investigators and intelligence personnel within and without the FBI, and as a resource for decision-makers elsewhere in the government. A 2004 threat assessment is scheduled to be released in April 2004.

We are preparing to produce, in the near future, the *FBI Daily Report* and the *FBI National Report* to provide daily intelligence briefings to personnel in the field and external customers. One will be produced at the classified level and limited in distribution to upper-level field managers. The other will be unclassified and widely distributed to field office personnel and our partners in the law enforcement community.

A good example of our ability to exploit evidence for its intelligence value and share that intelligence is our use of the al-Qa'ida terrorism handbook. A terrorism handbook seized from an al-Qa'ida location overseas in the mid-1990's was declassified and released by DOJ shortly after the events of September 11, 2001. We determined that intelligence gleaned from the handbook could provide useful guidance about al-Qa'ida's interests and capabilities. Accordingly, we produced and disseminated a series of intelligence products to share this intelligence with our personnel in the field and with our law enforcement partners. Nine Intelligence Bulletins were based in whole or in part on this intelligence. In addition, we used information derived from the al-Qa'ida Handbook to update our counterterrorism training, including the Intelligence Analyst Basic Course at the College of Analytical Studies, the Introduction to Counterterrorism Course at the National Academy, and sessions on Terrorism Indicators and Officer Safety in our SLATT training. The unclassified version of the handbook is now maintained as a reference in the FBI Library and is accessible to all the students at the Academy. It also is included in the reference manual CD-Rom distributed as part of SLATT training.

Quality of Daily Counterterrorism Briefings

One telling measure of our improved counterterrorism operations is the development of our capability to brief the daily terrorist threat information. The development of this capability reflects the maturing of our centralized Counterterrorism Program.

Prior to September 11, 2001, the FBI lacked the capacity to provide a comprehensive daily terrorism briefing – to assemble the current threat information, to determine what steps were being taken to address each threat, and to present a clear picture of each threat and the Bureau's response to that threat to the Director, senior managers, the Attorney General, and to others in the Administration who make operational and policy decisions. With a decentralized program in which investigations were run by individual field offices, the Bureau never had to develop this specialized skill. With the need for centralized management after September 11, 2001, however, it became an imperative.

Initial Capabilities

In the aftermath of the September 11, 2001, attacks, we were asked to begin sending to the White House each morning daily reports on counterterrorism-related events. We had no mechanism in place for collecting that information, so preparation of the reports was initially haphazard. For the first few months, the Director's Chief of Staff was responsible for preparing the daily report that would be delivered to the President. Throughout the day, he monitored developments, gathered urgent reports, attended briefings, and noted any item that might be worth including in the next morning's report. If there were questions he thought needed answering, he would either contact the appropriate person or ask SIOC to follow up and e-mail him an answer by 4:00 a.m. the next morning. He would arrive at 4:30 in the morning and update that morning's report based on any other overnight reports in SIOC and any e-mails that had come in overnight.

CT Watch then took that report and packaged it in a daily briefing book. Working with limited personnel, unreliable color printers, and few supplies, they managed to produce 15 to 20 briefing booklets per day.

New Capabilities

During the past 31 months, with the assistance of veterans from the Intelligence Community, we have established the infrastructure and the cadre of professionals to produce effective daily briefings and to share briefing materials more widely within the Bureau and with our partners.

In 2002 we established the Presidential Support Group within the Counterterrorism Division to prepare daily briefing materials. In the summer of 2003, this group was renamed the Strategic Analysis Unit and moved to the Office of Intelligence. Beginning in August 2003, the Strategic Analysis Unit began producing the Director's Daily Report *(DDR)*, a daily intelligence briefing that includes information on counterterrorism operations, terrorism threats, and information related to all areas of FBI investigative activity. To produce the DDR, the Strategic Analysis Unit consolidates and refines information provided in a standardized format by intelligence personnel in each division. Each morning, information about new threats is added, and information about threats that have been thoroughly vetted during the night is removed. The DDR is produced Monday through Friday and is distributed to executives in all operational divisions. The Director uses the DDR to brief the President nearly every weekday morning. The FBI also produces the *Presidential Intelligence Assessment*, a finished FBI intelligence product covering topics of particular interest to the President, and its personnel at TTIC contribute to the formulation of the daily *President's Terrorist Threat Report*.

Director Mueller holds threat briefings twice a day: an intelligence briefing at 7:15 a.m. and a case-oriented briefing at 5 p.m. At these briefings, a briefer and the operational executive managers provide a summary of the current threats and our operations. With CIA and DHS representatives in attendance, these meetings also serve to ensure that all threat information is appropriately passed to those agencies.

The development of this daily briefing operation is a tangible measure of the progress we have made since the day when terrorism investigations were run by individual field offices and little effort was made to centrally direct or coordinate them throughout the Bureau and with the other agencies involved in protecting the U.S. against terrorism.

Effectiveness of Counterterrorism Operations

The Bureau historically measured its performance, to a large extent, by the number of criminals it arrested. While useful for traditional law enforcement, where the primary objective is arrest and prosecution, this standard is under-inclusive as applied to counterterrorism, where the primary objective is to neutralize terrorist threats. It only captures that subset of terrorist threats that are neutralized by arresting terrorists and prosecuting them with charges of criminal terrorism. It fails to capture the terrorist threats we neutralize through means other than formal terrorism prosecutions – such as deportation, detention, arrest for non-terrorism charges, seizure of financial assets, and the sharing of information with foreign governments for their use in taking action against terrorists within their borders.

A more useful measure is one we have used in organized crime cases – the number of disruptions and dismantlements. This measure counts every time we – either by ourselves or with our partners in the law enforcement and intelligence communities – conduct an operation which disables, prevents, or interrupts terrorist fundraising, recruiting, training, or operational planning. Since September 11, 2001, the FBI has participated in dozens of such operations, disrupting a wide variety of domestic and international terrorist undertakings.

While the number of disruptions is significant, the most telling measure of our progress is the manner in which we have conducted individual operations consistent with our prevention mission. The extent of our transformation is most clearly seen in the approach we take when confronting specific terrorist threats. Our approach to these operations demonstrates the extent to which coordination and prevention through the development of actionable intelligence have become our guiding operational principles.

The following is a sampling of our investigative activities that show the various dimensions of our counterterrorism capabilities. The particulars of the first two operations have been publicly discussed, and the last two have resulted in criminal charges and have thereby been made public. While we have briefed Congressional Committees and the Commission on other investigations and terrorist disruptions that resulted in no criminal prosecutions and have thus remained classified, we cannot discuss them in this unclassified document.

The first two examples show our coordinated responses to periods of heightened threat.

End of Summer Task Force

During the investigation into the May 12, 2003, bombings in Riyadh, Saudi Arabia, significant intelligence was developed suggesting the existence of a plot to attack the U.S. homeland. This information, combined with other threat indicators, pointed to an increased threat of terrorist attacks for the end of summer.

- In response, we established the "End of Summer Task Force" made up of agents and analysts to examine the threat. The Task Force worked closely with other members of the Intelligence Community to coordinate operational and intelligence elements.

- FBI and Intelligence Community entities held bi-weekly meetings to share significant findings, operational information, and intelligence assessments.

- The Task Force met with document exploitation experts from the FBI and other Intelligence Community agencies to discuss the exploitation, dissemination, and tracking of leads from materials seized in the raids in Saudi Arabia in May and June of 2003.

- The Task Force received quality analytical assessments that were produced through timely information sharing between all the agencies involved, regular meetings and consultation among analysts from all the agencies, and close peer-to-peer coordination of analytic assessments across those agencies.

Response to Terrorist Threats Over the 2003 Holiday Season

In December 2003, the U.S. Intelligence Community became concerned about the possibility of near-term attacks in the homeland from al-Qa'ida. Strategic and tactical intelligence pointed to the possibility of attacks during the holiday season, and raised concerns about the use of foreign flights, threats to the energy sector, and the possibility of chemical, biological, radiological, or nuclear attacks. The FBI response was quick, thorough, based on centrally controlled, intelligence-based investigations, and focused on disrupting possible terrorist activity in the homeland.

We undertook the following steps to address the heightened threat environment:

- As soon as FBI Headquarters received the threat information, we immediately stood up a command post in SIOC to provide around-the-clock threat analysis and to maintain contact with appropriate JTTFs and Legal Attaché offices.

- Counterterrorism analysts immediately began a full review of all Sunni and Shia international terrorism cases from the past six months to determine if there were any previously unrecognized links. We used all the software search tools at our disposal, including link analysis, to ensure that there was no evidence of a connection to any existing terrorism case.

- We directed all 56 FBI field offices to take specific actions, including standing up 24/7 command posts, gathering intelligence through interviews and other means, and working with local agencies to increase security, share information, and assist the investigation.

- Senior Headquarters executives, including the Director, the Deputy Director, and CTD managers, regularly communicated with the SACs in each of the affected field offices via secure video teleconferencing.

- We issued several bulletins and advisories relating to these threats to state and municipal law enforcement.

- We established a Headquarters task force to vet the passenger manifests of certain in-bound and out-bound flights to identify potential terrorists. Representatives from DHS, CIA, and NSA met at FBI Headquarters and established a protocol for vetting flight manifests through the NJTTF. Task force members used the FBI data warehouse and NSA, CIA, and Bureau of Immigration and Customs Enforcement *(ICE)* databases in the vetting process.

- The NJTTF facilitated frequent communications with domestic and foreign intelligence and law enforcement partners. We regularly met with representatives of the French and

British governments during the threat period, and we gave them demonstrations of the manifest vetting system.

- We sent information from Headquarters to field offices and JTTFs with "tear sheets" to facilitate information sharing with local law enforcement.

- JTTFs in those cities determined to be at particular risk took additional proactive steps, maintained enhanced liaison with federal partners and certain private sector interests, and kept Headquarters managers advised of their activities through daily reports and video conferences.

Our multi-faceted, proactive response to this holiday threat environment highlights many of our reforms. We centrally coordinated our operations from Headquarters with regular contact with the field. We increased personnel levels to staff command posts and task forces at Headquarters and throughout the field. We relied on our information technology – our software search tools and consolidated databases – to analyze and quickly share the relevant information. We worked closely with our foreign, federal, state, and local partners in assessing and responding to the threat indicia. And, on January 29 and 30, 2004, we organized and sponsored an after-action review with representatives from CTD, the NJTTF, other federal agencies, and several foreign services to assess our response and identify lessons that will help us improve our response to future threat periods.

Iyman Faris

The investigation of Iyman Faris is a good example of how the FBI works cooperatively with our partners to investigate and neutralize a specific threat. This investigation was initiated and developed as a result of close coordination with our international, federal, state, and municipal partners.

Faris initially came to our attention when information from a foreign source linked Faris to terrorists who had plotted attacks to coincide with Millennium celebrations. With help from FBI Headquarters, agents and other JTTF members in our Cincinnati field office undertook an extensive investigation and ultimately interviewed Faris in March 2003. During the interview, Faris admitted that he had personal contact with several individuals tied to terrorism. At about the same time, another foreign source indicated that an Ohio-based truck driver had been tasked to attack U.S. bridges, and particularly the Brooklyn Bridge. Once that information came together, we quickly composed a targeted plan for Faris' interview team, assigned operational leads to field offices and JTTFs around the country, and teamed up with NYPD investigators and analysts.

As a result of these activities, Faris was arrested, and he ultimately pled guilty to the charge of Providing Material Support or Resources to a Designated Foreign Terrorist Organization. On October 28, 2003, Faris was sentenced to 20 years in prison. He has been interviewed subsequent to his sentencing as part of his cooperation agreement with the government.

Investigation of Criminal Enterprises Supporting Hizballah

As discussed above, a critical part of our counterterrorism strategy is the use of traditional criminal investigation and prosecution to disrupt terrorist activity. A good example is the recent joint investigation targeting criminal enterprises that raise money to support Hizballah, a foreign terrorist organization. To support Hizballah, these criminal enterprises, primarily based in the Detroit area, are engaged in a wide range of offenses, including credit card fraud, bank fraud, mail fraud, mortgage fraud, wire fraud, bankruptcy fraud, money laundering, contraband cigarette trafficking, trafficking in counterfeit cigarette tax stamps, transportation of stolen property, and trafficking in counterfeit goods.

A team made up of investigators from several FBI JTTFs, Legal Attachés, and our partner agencies has used an integrated strategy of intelligence collection and criminal investigative techniques to identify, disrupt, and defeat Hizballah support networks. To date, that strategy has produced 18 complaints, 37 indictments, 19 arrests, and 10 convictions. Here are two recent developments in that investigation:

- In January 2004, Elias Mohamad Akhdar of Dearborn, Michigan, was sentenced to 70 months in prison after pleading guilty to violations of the Racketeer Influenced and Corrupt Organizations Act *(RICO)* for his role in running a multi-million dollar enterprise involved in the smuggling of untaxed and low-taxed cigarettes between Michigan, North Carolina, and the Cattarangus Indian Reservation in New York. The Akhdar enterprise, which resulted in the evasion of approximately $2 million in Michigan state cigarette taxes, had two connections to Hizballah. First, one of the largest suppliers of contraband cigarettes to the racketeering conspiracy was Mohamad Hammoud of the Charlotte, North Carolina, Hizballah Cell, who was convicted of providing material support to Hizballah. Also, Hassan Moussa Makki, a key player in this enterprise, pled guilty in September 2003 to providing material support to Hizballah.

- In January 2004, Mahmoud Youssef Kourani, formerly of Dearborn, Michigan was indicted for Conspiracy to Provide Material Support to Hizballah. Kourani is charged with conspiring with his brother, the Hizballah Chief of Military Security for Southern Lebanon, and other unnamed co-conspirators to provide material support to Hizballah. Kourani is an alleged member, fighter, recruiter, and fundraiser for Hizballah. If convicted, he faces a maximum penalty of 15 years' imprisonment and a $250,000 fine.

Respect for Civil Liberties

It is the FBI's job to protect Americans, not only from crime and terrorism, but also from incursions into their constitutional rights. That effort starts with our own commitment to scrupulously protect privacy rights and civil liberties in the course of our investigations. With the tragedy of September 11, 2001, and the ensuing imperative to protect America against further attack, some questioned whether the Bureau would forsake civil liberties and personal privacy rights for the sake of investigative expediency. Thanks to the professionalism of our personnel and the respect for civil liberties institutionalized within the Bureau, our operations of the past 31 months have been carried out with full adherence to the Constitution and the principles of personal liberty and privacy.

The reason for this strict adherence to civil liberties lies in the regime of oversight, legal limitations and self-regulation that governs our investigative activities within the U.S. This regime is comprehensive, and it has many facets, including the following:

Statutory Limitations:

The following statutes, among others, help to guarantee that the Bureau's operations remain clearly within the bounds of the Constitution and of propriety:

- **The Foreign Intelligence Surveillance Act of 1978**—This law established a process for obtaining judicial approval of electronic surveillance and physical searches for the purpose of collecting foreign intelligence information.
- **The Whistleblower Protection Acts of 1989 and 1998**—These laws protect whistleblowers from retaliation.
- **The Freedom of Information Act of 1966**—This law provides the public with effective access to all FBI documents not covered by a specific statutory exemption.
- **The Privacy Act of 1974**—This law forbids the FBI and other federal agencies from collecting information about how individuals exercise their First Amendment rights, unless that collection is expressly authorized by statute or by the individual, or is pertinent to and within the scope of an authorized law enforcement activity.

Oversight Mechanisms:

- **Congressional Oversight—**Committees of the U.S. Congress, primarily the House and Senate Judiciary, Intelligence, Appropriations, and Government Reform/Governmental Affairs Committees, have broad oversight authority over the FBI. These committees – along with others – exercise regular, vigorous oversight into all aspects of the FBI's operations. This oversight has significantly increased in breadth and intensity since the 1970's, and it provides important additional assurance that the FBI conducts its investigations in accordance with the law and the Constitution.
- **Counterintelligence Oversight—**The FBI's counterintelligence operations are subject to significant outside oversight beyond that conducted by Congress. DOJ's Office of Intelligence Policy and Review, which was established in 1981 as required by Executive Order 12333, monitors intelligence and counterintelligence investigations conducted by U.S. intelligence agencies and provides Congress a series of semi-annual reports on various aspects of the FBI's counterintelligence operations. The FBI also is subject to oversight by the Intelligence Oversight Board. Established in 1993, the Intelligence Oversight Board is comprised of four members appointed from the membership of the President's Foreign Intelligence Advisory Board. Among its other responsibilities, the Intelligence Oversight Board reviews all violations of national security law, Executive Order or Presidential Decision Directive by the FBI and the other intelligence agencies, and issues reports thereon to the President and the Attorney General.

Self-Regulation and Enforcement:

- **Attorney General's Crimes Guidelines—**The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations *(General Crimes Guidelines)* have been in effect, in one form or another, since the mid-1970's. These Guidelines govern all investigations by the FBI of crimes and crime-related activities. They set forth the standards and requirements under which an investigation may be initiated, and they define the permissible scope, duration, subject matters, and objectives of an FBI criminal investigation. They are designed to provide Special Agents with a framework that maintains the proper balance between the public's need for effective law enforcement and terrorism prevention, on the one hand, and the preservation of individual rights and liberties, on the other. Among the provisions that specifically serve to protect individual rights are the following: **1)** the prohibition against initiating investigations directed solely at the exercise of First Amendment rights or other constitutionally protected activity; and **2)** the requirement that agents consider using the least intrusive method necessary to achieve their investigative goals. In short, the Guidelines translate the Department's respect for individual rights and liberties into practical policy, and thereby prevent investigative abuses.
- **Attorney General's National Security/Foreign Intelligence Guidelines—**The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection *(National Security Guidelines)* were first issued in 1976, and recently updated in October 2003. These classified guidelines govern the manner in which the FBI conducts its counterintelligence investigations – those investigations that focus on protecting the U.S. from external threats. The National Security Guidelines, like the domestic General Crimes Guidelines, were designed to maintain the proper balance between the public's need for effective counterintelligence and the imperative to respect and protect individual rights. The National Security Guidelines contain a number of provisions designed to ensure that individual rights and liberties will be protected, such as the prohibition on investigations of First Amendment activities and the rule that a U.S. person may be the subject of a counterintelligence investigation only if circumstances indicate that he or she might be acting for or on behalf of a foreign power.
- **Internal Enforcement—**The FBI's Office of Professional Responsibility and the DOJ's Office of the Inspector General investigate allegations of misconduct.
- **Internal Safeguards—**Internal safeguards include the Privacy Council, which reviews the plans of any record system that is proposed within the FBI for compliance with the Privacy Act and related privacy policies, and the Criminal Undercover Operations Review Committee, which is comprised of senior DOJ and FBI officials and reviews all proposed undercover operations that involve sensitive circumstances. There also is a Criminal Informant Review Committee, comprised of senior FBI and DOJ officials, which provides oversight over several categories of human sources, such as high-level criminal informants and long-term sources.

- **Training—**The Bureau's training program emphasizes respect for the constitutional rights and dignity of individuals. Agents receive extensive instruction on constitutional law and criminal procedure, and all new agents visit the Holocaust Museum to learn the consequences of government oppression and persecution. Then, throughout their careers, agents receive quarterly training from the Chief Division Counsel in each field office to keep them up to speed on the latest guidelines, changes to laws and regulations, and judicial decisions related to constitutional rights and liberties.

This comprehensive infrastructure of legal limitations, oversight and self-regulation effectively ensures that the Bureau's operations always are carried out within Constitutional and statutory parameters.

A number of outside entities and individuals have studied our operations since September 11, 2001, and have found no indication that we have conducted them with less than full regard for civil liberties. The DOJ's Inspector General, for example, has issued three semi-annual reports, indicating that his office had received no complaints for each six month period alleging misconduct by DOJ employees related to their use of a substantive provision in the USA PATRIOT Act.

At an October 21, 2003, hearing of the Senate Committee on the Judiciary regarding the use of USA PATRIOT Act authorities, one senator said that "the tide of criticism" being directed against the USA PATRIOT Act "is both misinformed and overblown," and that the Justice Department has "done a pretty good job in terms of implementing" the law's provisions. Another senator said, "I have never had a single abuse of the Patriot Act reported to me. My staff e-mailed the ACLU and asked them for instances of actual abuses. They e-mailed back and said they had none."

Similarly, the General Accounting Office *(GAO)* examined our implementation of the new Attorney General Guidelines. In its June 18, 2003, report on FBI Reorganization, the GAO found that there were no reported allegations that appeared to involve noncompliance with or abuse of the new investigative authorities granted under the Guidelines.

We take great pride in our record of protecting both civil liberties and national security since September 11, 2001. It is a testament to the vitality of the existing regime of constitutional, legal and regulatory protections and to the commitment of individual Bureau employees to the protection of individual rights.

CONCLUSION

The September 11, 2001, attacks awakened all of us to the deadly threat of modern terrorism and to the need for bold action. We in the FBI have undertaken that bold action over the past 31 months. While there is still much work to be done, we have made significant progress with the reform efforts described in the foregoing report. With these efforts, and with the unwavering support of the American people, we are confident that we will prevail in our war against terrorism.

Director's Note

The transformation described above has been a tremendous effort, and the dedicated men and women of the FBI deserve great credit for the progress we have made. FBI personnel have consistently sacrificed and placed duty over self-interest as they have embraced the Bureau's new mission and adapted to the necessary changes. Their professionalism has made this transformation possible. I cannot thank them enough.